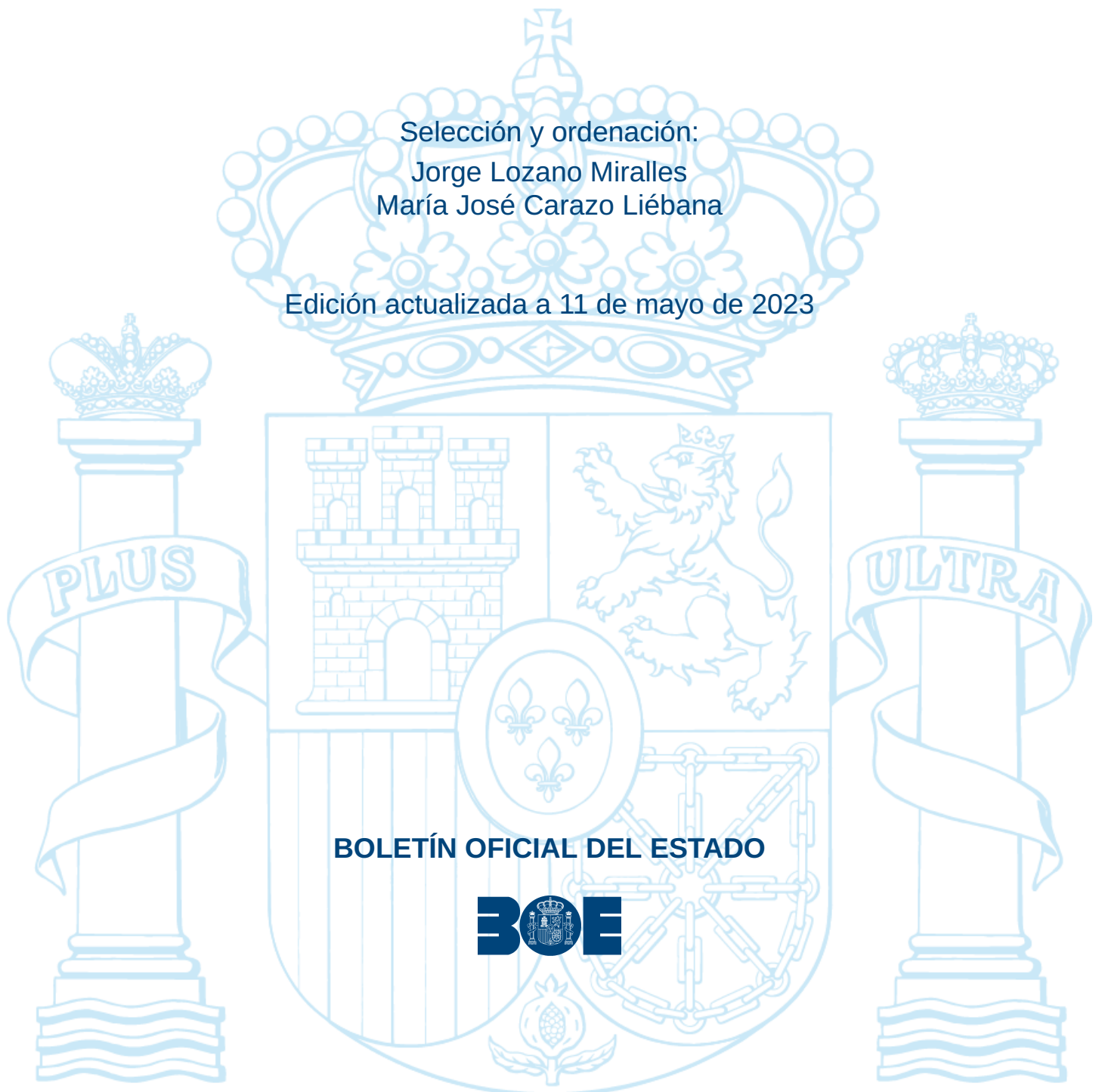


Códigos electrónicos

Ámbitos de la Seguridad Nacional: Ciberseguridad

Selección y ordenación:
Jorge Lozano Miralles
María José Carazo Liébana

Edición actualizada a 11 de mayo de 2023





La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es

@ Agencia Estatal Boletín Oficial del Estado

NIPO (PDF): 090-20-225-2

NIPO (Papel): 090-20-224-7

NIPO (ePUB): 090-20-226-8

ISBN: 978-84-340-2678-0

Depósito Legal: M-28050-2020

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

SUMARIO

I. PROTECCIÓN DE DATOS

§ 1. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos	1
§ 2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	26
§ 3. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales	88
§ 4. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. [Inclusión parcial]	135
§ 5. Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones	138
§ 6. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]	157
§ 7. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras	165
§ 8. Resolución de 9 de marzo de 2016, de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, por la que se crea el fichero de datos de carácter personal "Registro de grupos de interés"	170

II. CIBERAMENAZAS Y SEGURIDAD EN EL CIBERESPACIO. COOPERACIÓN EN MATERIA DE SEGURIDAD

§ 9. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información	172
§ 10. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información	193
§ 11. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	218
§ 12. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social	294
§ 13. Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad	297

§ 14. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional	302
--	-----

III. INFRAESTRUCTURAS CRÍTICAS EN ESPAÑA

§ 15. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos	320
§ 16. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas	339
§ 17. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas	350

IV. USO EFICIENTE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

§ 18. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad . . .	368
--	-----

ÍNDICE SISTEMÁTICO

I. PROTECCIÓN DE DATOS

§ 1. Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos	1
<i>Preámbulo</i>	1
<i>Artículos</i>	4
<i>Disposiciones adicionales</i>	4
<i>Disposiciones transitorias</i>	4
<i>Disposiciones derogatorias</i>	4
<i>Disposiciones finales</i>	4
ESTATUTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS	5
CAPÍTULO I. Disposiciones generales	5
CAPÍTULO II. Estructura orgánica de la Agencia Española de Protección de Datos	8
Sección 1. ^a De la Presidencia de la Agencia Española de Protección de Datos	8
Sección 2. ^a La Adjuntía a la Presidencia de la Agencia Española de Protección de Datos	10
Sección 3. ^a Procedimiento de designación de la Presidencia y la Adjuntía	11
Sección 4. ^a El Consejo Consultivo de la Agencia Española de Protección de Datos	13
Sección 5. ^a Otros órganos directamente dependientes de la Presidencia de la Agencia Española de Protección de Datos	14
CAPÍTULO III. Personal al servicio de la Agencia Española de Protección de Datos	20
CAPÍTULO IV. Régimen económico, presupuestario, patrimonial y de contratación	22
Sección 1. ^a Régimen económico-financiero, patrimonial y de contratación	22
Sección 2. ^a Régimen presupuestario, de contabilidad y control económico-financiero	23
CAPÍTULO V. Asesoramiento jurídico de la Agencia Española de Protección de Datos	25
§ 2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales	26
<i>Preámbulo</i>	26
TÍTULO I. Disposiciones generales	33
TÍTULO II. Principios de protección de datos	34
TÍTULO III. Derechos de las personas	36
CAPÍTULO I. Transparencia e información	36
CAPÍTULO II. Ejercicio de los derechos	37
TÍTULO IV. Disposiciones aplicables a tratamientos concretos	38
TÍTULO V. Responsable y encargado del tratamiento	42
CAPÍTULO I. Disposiciones generales. Medidas de responsabilidad activa	42
CAPÍTULO II. Encargado del tratamiento	44
CAPÍTULO III. Delegado de protección de datos	45
CAPÍTULO IV. Códigos de conducta y certificación	47
TÍTULO VI. Transferencias internacionales de datos	48
TÍTULO VII. Autoridades de protección de datos	49
CAPÍTULO I. La Agencia Española de Protección de Datos	49
Sección 1. ^a Disposiciones generales	49
Sección 2. ^a Potestades de investigación y planes de auditoría preventiva	53
Sección 3. ^a Otras potestades de la Agencia Española de Protección de Datos	55
CAPÍTULO II. Autoridades autonómicas de protección de datos	56
Sección 1. ^a Disposiciones generales	56
Sección 2. ^a Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679	57
TÍTULO VIII. Procedimientos en caso de posible vulneración de la normativa de protección de datos	57
TÍTULO IX. Régimen sancionador	61

§ 6. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]	157
[...]	
TÍTULO II. De la actividad de las Administraciones Públicas	157
CAPÍTULO I. Normas generales de actuación.	157
[...]	
TÍTULO III. De los actos administrativos	162
[...]	
CAPÍTULO II. Eficacia de los actos.	162
[...]	
TÍTULO IV. De las disposiciones sobre el procedimiento administrativo común.	163
[...]	
CAPÍTULO III. Ordenación del procedimiento	163
[...]	
<i>Disposiciones adicionales</i>	163
§ 7. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras	165
<i>Preámbulo</i>	165
<i>Artículos</i>	167
<i>Disposiciones transitorias</i>	168
<i>Disposiciones finales</i>	168
ANEXO. 1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.	168
§ 8. Resolución de 9 de marzo de 2016, de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, por la que se crea el fichero de datos de carácter personal "Registro de grupos de interés"	170
<i>Preámbulo</i>	170
<i>Artículos</i>	171
ANEXO I. Creación de ficheros.	171
II. CIBERAMENAZAS Y SEGURIDAD EN EL CIBERESPACIO. COOPERACIÓN EN MATERIA DE SEGURIDAD	
§ 9. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información	172
<i>Preámbulo</i>	172
TÍTULO I. Disposiciones generales	176
TÍTULO II. Servicios esenciales y servicios digitales	178
TÍTULO III. Marco estratégico e institucional	179
TÍTULO IV. Obligaciones de seguridad	182
TÍTULO V. Notificación de incidentes	184
TÍTULO VI. Supervisión	187
TÍTULO VII. Régimen sancionador	188
<i>Disposiciones adicionales</i>	191
<i>Disposiciones finales</i>	192

§ 10. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información	193
<i>Preámbulo</i>	193
CAPÍTULO I. Disposiciones generales	195
CAPÍTULO II. Marco estratégico e institucional	196
CAPÍTULO III. Requisitos de seguridad	199
CAPÍTULO IV. Gestión de incidentes de seguridad.	201
CAPÍTULO V. Supervisión	204
<i>Disposiciones adicionales</i>	205
<i>Disposiciones transitorias</i>	206
<i>Disposiciones finales</i>	206
ANEXO. Instrucción nacional de notificación y gestión de ciberincidentes	207
§ 11. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	218
<i>Preámbulo</i>	218
CAPÍTULO I. Disposiciones generales	225
CAPÍTULO II. Principios básicos	226
CAPÍTULO III. Política de seguridad y requisitos mínimos de seguridad	228
CAPÍTULO IV. Seguridad de los sistemas: auditoría, informe e incidentes de seguridad	234
CAPÍTULO V. Normas de conformidad	236
CAPÍTULO VI. Actualización del Esquema Nacional de Seguridad.	237
CAPÍTULO VII. Categorización de los sistemas de información	237
<i>Disposiciones adicionales</i>	238
<i>Disposiciones transitorias</i>	238
<i>Disposiciones derogatorias</i>	238
<i>Disposiciones finales</i>	239
ANEXO I. Categorías de seguridad de los sistemas de información.	239
ANEXO II. Medidas de Seguridad	241
ANEXO III. Auditoría de la seguridad	289
ANEXO IV. Glosario	290
§ 12. Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social.	294
<i>Preámbulo</i>	294
<i>Artículos</i>	295
<i>Disposiciones adicionales</i>	296
<i>Disposiciones finales</i>	296
§ 13. Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad	297
<i>Parte dispositiva</i>	297
ANEJO. Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad	297
ANEXO. Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad	298
§ 14. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional	302
<i>Parte dispositiva</i>	302
ANEXO. Estrategia Nacional de Ciberseguridad 2019	302
Resumen ejecutivo	303
Introducción	304
CAPÍTULO 1. El ciberespacio como espacio común global	305
CAPÍTULO 2. Las amenazas y desafíos en el ciberespacio	307
CAPÍTULO 3. Propósito, principios y objetivos para la ciberseguridad.	309
CAPÍTULO 4. Líneas de acción y medidas	313
CAPÍTULO 5. La ciberseguridad en el Sistema de Seguridad Nacional	317

III. INFRAESTRUCTURAS CRÍTICAS EN ESPAÑA

§ 15. Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos	320
<i>Parte dispositiva</i>	320
ANEXO I. Guía Contenidos Mínimos	321
ANEXO II. Guía de contenidos mínimos	330
§ 16. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas	339
<i>Preámbulo</i>	339
TÍTULO I. Disposiciones generales	341
TÍTULO II. El Sistema de Protección de Infraestructuras Críticas	343
TÍTULO III. Instrumentos y comunicación del Sistema	346
<i>Disposiciones adicionales</i>	347
<i>Disposiciones finales</i>	348
ANEXO. Sectores estratégicos y Ministerios/Organismos del sistema competentes	349
§ 17. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas	350
<i>Preámbulo</i>	350
TÍTULO I.	351
<i>Disposiciones transitorias</i>	351
<i>Disposiciones finales</i>	351
REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS	352
TÍTULO I. Disposiciones generales	352
CAPÍTULO I. Objeto y ámbito de aplicación	352
CAPÍTULO II. El Catálogo Nacional de Infraestructuras Estratégicas	352
TÍTULO II. Los agentes del Sistema de Protección de Infraestructuras Críticas	353
TÍTULO III. Instrumentos de planificación	360
CAPÍTULO I. El Plan Nacional de Protección de las Infraestructuras Críticas	360
CAPÍTULO II. Los Planes Estratégicos Sectoriales	361
CAPÍTULO III. Los Planes de Seguridad del Operador	362
CAPÍTULO IV. Los Planes de Protección Específicos	363
CAPÍTULO V. Los Planes de Apoyo Operativo	365
TÍTULO IV. Comunicaciones entre los operadores críticos y las Administraciones públicas	366

IV. USO EFICIENTE DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

§ 18. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	368
<i>Preámbulo</i>	368
CAPÍTULO I. Disposiciones generales	375
CAPÍTULO II. Principios básicos	376
CAPÍTULO III. Política de seguridad y requisitos mínimos de seguridad	378
CAPÍTULO IV. Seguridad de los sistemas: auditoría, informe e incidentes de seguridad	384
CAPÍTULO V. Normas de conformidad	386
CAPÍTULO VI. Actualización del Esquema Nacional de Seguridad	387
CAPÍTULO VII. Categorización de los sistemas de información	387
<i>Disposiciones adicionales</i>	388
<i>Disposiciones transitorias</i>	388
<i>Disposiciones derogatorias</i>	388
<i>Disposiciones finales</i>	389
ANEXO I. Categorías de seguridad de los sistemas de información	389
ANEXO II. Medidas de Seguridad	391
ANEXO III. Auditoría de la seguridad	439

ANEXO IV. Glosario 440

§ 1

Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 131, de 2 de junio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-9175

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, encomendó el control de la aplicación de sus disposiciones a un ente público independiente al que denominó Agencia de Protección de Datos y que se caracterizaba por la absoluta independencia de su Director en el ejercicio de sus funciones, reforzada por el establecimiento de un mandato fijo que solo podía ser acortado por un *numerus clausus* de causas de cese. La efectiva creación de la Agencia se llevó a cabo mediante la regulación de su estructura orgánica y la aprobación de su Estatuto por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Posteriormente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobada para transponer a nuestro Derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mantuvo la configuración de la Agencia como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

En el momento actual, el régimen jurídico de la protección de datos de carácter personal viene establecido directamente por el Derecho de la Unión Europea tras la plena aplicación, desde el 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Dicho Reglamento fue adoptado con dos claros objetivos: por una parte, superar la fragmentación existente en la aplicación de las normas de trasposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que ha dado lugar, en la práctica, y a pesar de derivar todos ellos de unos principios comúnmente aceptados, a la existencia de tantos regímenes de protección de datos como Estados Miembros, con distintos niveles de protección y, especialmente, de reacción ante conductas que pudieran suponer una infracción de la norma. Y por otra, adaptar las normas de protección de datos a la rápida evolución tecnológica y a los fenómenos derivados del desarrollo exponencial de la sociedad de la información y la globalización que la misma conlleva en el tratamiento de los datos de carácter personal.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa, al evolucionar desde el antiguo modelo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que estaba basado en una serie de obligaciones a las que los responsables y encargados del tratamiento habían de sujetarse, unidas al reconocimiento de potestades reactivas de las autoridades de protección de datos, hacia un nuevo paradigma basado en lo que se denomina «enfoque de riesgo»; es decir, en la necesaria evaluación por los propios responsables y encargados del tratamiento de los riesgos que su actividad puede generar en el derecho fundamental para, a partir de esa valoración, adoptar las medidas que resulten necesarias para mitigarlos en todo lo que sea posible. Se evoluciona así hacia un modelo de responsabilidad activa, que exigirá a su vez una valoración dinámica de la actividad desarrollada por el sujeto obligado por la norma y la adopción de medidas tales como la privacidad desde el diseño y por defecto, la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnicas y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento. En este modelo, por otra parte, las medidas de carácter organizativo, tales como la designación de un delegado de protección de datos, sobre el que recae la función de asesorar y supervisar las actividades de tratamiento de los responsables o encargados, adquieren un papel fundamental para la salvaguarda del derecho fundamental de los afectados. Finalmente, se fomenta el establecimiento de sistemas de autorregulación, incluyendo mecanismos de resolución extrajudicial de controversias, y el desarrollo de esquemas de certificación.

El nuevo modelo de protección de datos de carácter personal tiene una incidencia notable en la organización y funciones tradicionales de la Agencia Española de Protección de Datos, puesto que el Reglamento general de protección de datos refuerza las competencias de las autoridades de control que deberán contar con todos las funciones y poderes efectivos, incluidos los poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos previstos en el propio Reglamento y ha introducido los mecanismos que garanticen la necesaria coordinación y coherencia entre las diferentes autoridades de control europeas.

Para ello, el Reglamento inviste a las autoridades de protección de datos de una total independencia, destacando en el considerando 117 que «el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa».

A estos efectos, el citado Reglamento impone a los Estados miembros la adopción de un régimen jurídico específico que deberá establecerse mediante ley respecto de todos los elementos que recoge en su artículo 54.

Para dar cumplimiento a dicha obligación se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuyo título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se han de establecer por ley nacional, configurando la Agencia Española de Protección de Datos como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

Asimismo, atribuye a la Agencia Española la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos e introduce una serie de modificaciones en su régimen jurídico con el fin de reforzar su independencia, destacando, entre otras, las relativas al procedimiento de nombramiento, mandato y cese de la Presidencia y de la Adjuntía a la Presidencia, quienes ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño; el régimen de modificaciones y de vinculación de los créditos de su presupuesto; la elaboración y aprobación de la relación de puestos de trabajo;

la composición del Consejo Consultivo; el deber de colaboración con la Agencia; la realización de planes de auditoría o las potestades de regulación por medio de circulares.

Por otro lado, hay que tener en cuenta que la Agencia Española de Protección de Datos no solo ejerce las competencias derivadas del Reglamento, sino que también ejercerá las que establece la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Igualmente ejerce actualmente las potestades derivadas de la Directiva 2002/58 del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que en la actualidad se recogen en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y en la legislación en materia de telecomunicaciones.

Por todo ello, resulta necesario la aprobación de un nuevo Estatuto que adapte la organización y funcionamiento de la Agencia Española de Protección de Datos a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre.

El presente real decreto consta de un artículo único que aprueba el Estatuto de la Agencia Española de Protección de Datos, una disposición adicional sobre supresión de órganos directivos, una disposición transitoria única sobre unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general, una disposición derogatoria única y una disposición final única relativa a la entrada en vigor del real decreto.

El Estatuto se estructura en cinco capítulos. El primero de ellos incluye las disposiciones generales sobre la naturaleza, régimen jurídico, autonomía e independencia, funciones y potestades, circulares, acción exterior, colaboración en el ámbito de la Administración de Justicia, programación, memoria anual, sede y transparencia y publicidad.

En el capítulo II se define la estructura orgánica de la Agencia Española de Protección de Datos especificando las funciones de sus diferentes órganos. En concreto, la estructura orgánica se articula en torno a la Presidencia, de la que dependen la Adjuntía a la Presidencia, la Subdirección General de Inspección de datos, la Subdirección General de Promoción y Autorizaciones, la Secretaría General, la División de Relaciones Internacionales y la División de Innovación Tecnológica. Se regula el procedimiento de designación de la Presidencia y la Adjuntía, como consecuencia de una observación formulada al respecto por el Consejo de Estado en su dictamen sobre el proyecto. También se desarrolla el régimen, competencias y funcionamiento del Consejo Consultivo en cuanto órgano colegiado de asesoramiento de la Presidencia de la Agencia Española de Protección de Datos.

El capítulo III se refiere al personal al servicio de la Agencia Española de Protección de Datos, que podrá ser funcionario o laboral, a la elaboración y aprobación de la relación de puestos de trabajo, retribuciones, evaluación del desempeño, incompatibilidades y deber de secreto profesional.

El capítulo IV regula el régimen económico, presupuestario, patrimonial y de contratación, detallando el régimen económico financiero, patrimonial y de contratación y el régimen presupuestario, de contabilidad y control económico financiero.

Por último, el capítulo V regula el asesoramiento jurídico de la Agencia, que se encomienda a la Abogacía General del Estado-Servicio Jurídico del Estado en virtud del correspondiente convenio.

Este real decreto se adecua a los principios de buena regulación (necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia) conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa y la potestad reglamentaria, según establece el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Así, este real decreto atiende a la necesidad de adecuar la estructura orgánica de la Agencia Española de Protección de Datos a lo previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en la Ley Orgánica 7/2021, de 26 de mayo, y es eficaz y proporcionado en el cumplimiento de este propósito, sin afectar en forma alguna a los derechos y deberes de la ciudadanía. Asimismo, contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Agencia, al adecuarla a las nuevas competencias establecidas en

dichas normas. Cumple también con el principio de transparencia, y es también adecuada al principio de eficiencia, ya que, entre otras cuestiones, no impone cargas administrativas adicionales.

En su virtud, a propuesta de la Agencia Española de Protección de Datos, y a propuesta conjunta del Ministro de Política Territorial y Función Pública, de la Ministra de Hacienda y del Ministro de Justicia, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 1 de junio de 2021,

DISPONGO:

Artículo único. *Aprobación del Estatuto de la Agencia Española de Protección de Datos.*

De conformidad con lo dispuesto en el artículo 45.2 y en la disposición final decimoquinta de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se aprueba el Estatuto de la Agencia Española de Protección de Datos, que se inserta a continuación.

Disposición adicional única. *Supresión de órganos directivos.*

Quedan suprimidos los siguientes órganos directivos:

- a) El Director de la Agencia Española de Protección de Datos.
- b) El Registro General de Protección de Datos.
- c) La Inspección de Datos.

Disposición transitoria única. *Unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general.*

Las unidades y puestos de trabajo con el nivel orgánico inferior a subdirección general continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios hasta que se aprueben las correspondientes relaciones o catálogos de puestos de trabajo de la Agencia Española de Protección de Datos adaptados a la estructura orgánica de este real decreto.

Las unidades y puestos de trabajo encuadrados en los órganos suprimidos, o cuya dependencia orgánica haya sido modificada por este real decreto, se adscribirán provisionalmente, mediante resolución de la Presidencia de la Agencia Española de Protección de Datos, hasta tanto entren en vigor las correspondientes relaciones o catálogos de puestos de trabajo, a los órganos regulados en este real decreto en función de las atribuciones que estos tengan asignadas.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final única. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ESTATUTO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CAPÍTULO I

Disposiciones generales

Artículo 1. *Naturaleza.*

La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en el artículo 109 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

Artículo 2. *Sede.*

La Agencia Española de Protección de Datos tendrá su sede en Madrid.

Artículo 3. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sus disposiciones de desarrollo y el presente Estatuto.

2. Supletoriamente, en cuanto sea compatible con su plena independencia, se regirá por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en particular lo dispuesto para organismos autónomos; por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas; por la Ley 47/2003, de 26 de noviembre, General Presupuestaria; por la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014; por la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, así como el resto de las normas de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común.

3. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

4. La Agencia Española de Protección de Datos estará sujeta al principio de sostenibilidad financiera de acuerdo con lo previsto en la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

5. De conformidad con lo previsto en la disposición adicional vigésima de la Ley Orgánica 3/2018, de 5 de diciembre, no será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

6. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 95 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 4. Autonomía e independencia.

1. De conformidad con lo dispuesto en el artículo 52 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el ejercicio de sus funciones y para el cumplimiento de los fines que le han sido asignados, la Agencia Española de Protección de Datos cuenta con autonomía orgánica y funcional y actúa con plena independencia del Gobierno, de las Administraciones Públicas y de cualquier interés empresarial o comercial.

2. Ni el personal ni los miembros de los órganos de la Agencia Española de Protección de Datos podrán aceptar ni solicitar instrucciones de ninguna entidad pública o privada.

Artículo 5. Funciones y potestades.

1. Corresponde a la Agencia Española de Protección de Datos la función de supervisar la aplicación de la normativa vigente en materia de protección de datos personales con el fin de proteger los derechos y libertades de las personas físicas en lo que respecta al tratamiento y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, y en sus disposiciones de desarrollo.

2. Asimismo, le corresponde supervisar la aplicación de la normativa vigente en materia de garantía de los derechos digitales contemplados en los artículos 89 a 94 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. La Agencia Española de Protección de Datos colaborará con los órganos competentes en lo que respecta al desarrollo normativo y aplicación de las normas que incidan en materia propia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, y a tal efecto:

a) Informará preceptivamente los proyectos de disposiciones generales de desarrollo del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre.

b) Informará preceptivamente cualesquiera anteproyectos de ley o proyectos de reglamento que incidan en la materia propia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre.

c) Dictará circulares que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de la Ley Orgánica 3/2018, de 5 de diciembre, así como instrucciones y recomendaciones.

4. La Agencia Española de Protección de Datos ejercerá el control de la observancia de lo dispuesto en los artículos 4, 7 y 10 a 22 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, y en especial:

a) Informará con carácter preceptivo el contenido y formato de los cuestionarios, hojas censuales y otros documentos de recogida de datos con fines estadísticos.

b) Dictaminará sobre los procesos de recogida y tratamiento de los datos personales a efectos estadísticos.

c) Informará con carácter preceptivo los anteproyectos de ley por los que se exijan datos con carácter obligatorio y su adecuación a lo dispuesto en el artículo 7 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.

d) Dictaminará sobre las condiciones de seguridad de los tratamientos realizados con fines exclusivamente estadísticos.

5. La Agencia Española de Protección de Datos adoptará conjuntamente con el Consejo de Transparencia y Buen Gobierno, los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma.

6. Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 6. *Circulares de la Agencia Española de Protección de Datos.*

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, que se denominarán «Circulares de la Agencia Española de Protección de Datos» y que serán obligatorias una vez publicadas en el «Boletín Oficial del Estado».

2. El Proyecto de Circular se iniciará mediante un informe técnico, suscrito por la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos o el Subdirector General o Director de División correspondiente, que constará de las siguientes partes:

- a) Especificación de la norma o normas habilitantes para dictar la disposición.
- b) Justificación de la necesidad de la disposición, así como de las medidas o soluciones técnicas que se propongan y de los fines que se pretenden alcanzar.
- c) Proyecto de Circular.

3. Se elaborará también un informe jurídico o de legalidad, emitido por el Gabinete Jurídico de la Agencia Española de Protección de Datos.

4. En el procedimiento de elaboración de las circulares se dará audiencia a las personas titulares de derechos e intereses legítimos que resulten afectados por las mismas, directamente o a través de las organizaciones y asociaciones reconocidas por la ley que los agrupen o los representen y cuyos fines guarden relación directa con el objeto de la circular, y se fomentará la participación de los ciudadanos.

El trámite de audiencia e información pública se realizará mediante la publicación del texto en la página web de la Agencia y tendrá un plazo mínimo de quince días hábiles, que podrá ser reducido hasta un mínimo de siete días hábiles cuando razones debidamente motivadas así lo justifiquen. El trámite de audiencia e información pública solo podrá omitirse cuando existan graves razones de interés público, que deberán justificarse en el informe técnico.

5. Asimismo, podrá recabarse, cuando proceda, el parecer de los departamentos de la Administración General del Estado cuyas competencias puedan verse específicamente afectadas por la regulación proyectada.

6. Cumplidos los trámites anteriores, se remitirá, cuando no le hubiera correspondido la iniciativa, a la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos, quien podrá solicitar que se complete el expediente.

7. El proyecto de circular, acompañada de una memoria justificativa y del expediente, se elevará por la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos quien podrá solicitar otros informes sin perjuicio de los que resulten preceptivos.

8. Se recabará el dictamen del Consejo de Estado por conducto de la persona titular del Ministerio de Justicia.

9. Una vez concluidos los trámites precedentes, el proyecto de circular será sometido a la aprobación final de la Presidencia de la Agencia Española de Protección de Datos, sin que en ningún caso sea posible la delegación de esta facultad en ningún otro órgano.

10. Las circulares serán publicadas en el «Boletín Oficial del Estado» y entrarán en vigor conforme a lo previsto en el artículo 2 del Código Civil.

Artículo 7. *Acción exterior.*

Corresponderá a la persona titular de la Presidencia de la Agencia Española de Protección de Datos designar los representantes que deban formar parte de la autoridad de control común de protección de datos prevista en los Convenios Internacionales de los que España sea parte.

Artículo 8. *Colaboración en el ámbito de la Administración de Justicia.*

La Agencia Española de Protección de Datos y el Consejo General del Poder Judicial colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, les atribuye en materia de protección de datos de carácter personal en el ámbito de la Administración de Justicia.

Artículo 9. *Programación.*

La Presidencia de la Agencia Española de Protección de Datos aprobará, en el primer semestre de su nombramiento y con carácter quinquenal, un Plan Estratégico con el objetivo de sentar las bases de las líneas de actuación de la Agencia en dicho periodo, incorporando las acciones específicas que cada departamento de la misma haya propuesto en relación con sus respectivas materias, así como el calendario de las circulares que se prevean aprobar.

Artículo 10. *Memoria anual.*

1. La Agencia Española de Protección de Datos redactará una Memoria anual sobre la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de las demás disposiciones legales y reglamentarias sobre protección de datos, la cual comprenderá, además de la información necesaria sobre el funcionamiento de la Agencia:

a) Una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Un análisis y una valoración de los problemas de la protección de datos a escala nacional.

2. La Memoria anual se remitirá al Congreso de los Diputados, al Senado, al Gobierno, al Defensor del Pueblo y a las autoridades autonómicas de protección de datos, se pondrá a disposición de la Comisión Europea y del Comité europeo de protección de datos, y se publicará en la página web de la Agencia.

Artículo 11. *Transparencia y publicidad.*

1. La Agencia Española de Protección de Datos publicará en su página web las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, las que pongan fin a los procedimientos de reclamación, las que archiven las actuaciones previas de investigación, las que sancionen con apercibimiento a las entidades a que se refiere el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y las que impongan medidas cautelares.

2. Sin perjuicio de lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, será igualmente objeto de publicación en la página web toda aquella información que la Presidencia considere relevante y que contribuya al mejor cumplimiento de sus funciones.

CAPÍTULO II

Estructura orgánica de la Agencia Española de Protección de Datos

Sección 1.ª De la Presidencia de la Agencia Española de Protección de Datos

Artículo 12. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos tendrá la consideración de alto cargo, con rango de Subsecretario y será designada de conformidad con el procedimiento establecido en el artículo 48 de la Ley Orgánica 3/2018, de 5 de diciembre, y solo cesará por las causas que en el mismo se establecen.

2. La persona titular de la Presidencia poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. La persona titular de la Presidencia cesante continuará en funciones hasta la toma de posesión de la nueva persona titular de la Presidencia.

4. Es un cargo de dedicación exclusiva, está sujeto al régimen de incompatibilidades de los altos cargos de la Administración General del Estado, y será incompatible con el ejercicio de cualquier actividad pública o privada, retribuida o no, salvo las que sean inherentes a su condición de titular de la Presidencia de la Agencia Española de Protección de Datos.

5. Las retribuciones de la persona titular de la Presidencia se fijarán de acuerdo con lo dispuesto en el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades.

6. De la Presidencia depende directamente, como órgano directivo, la Adjuntía a la Presidencia.

7. Asimismo, dependen directamente de la Presidencia los siguientes órganos con nivel orgánico de subdirección general:

- a) La Subdirección General de Inspección de Datos.
- b) La Subdirección General de Promoción y Autorizaciones.
- c) La Secretaría General.

8. También dependen directamente de la Presidencia, con el nivel que se determine en la relación de puestos de trabajo, las siguientes divisiones:

- a) La División de Relaciones Internacionales.
- b) La División de Innovación Tecnológica.

Artículo 13. *Funciones de la Presidencia.*

1. Corresponde a la Presidencia de la Agencia Española de Protección de Datos:

- a) La dirección de la Agencia.
- b) Ostentar su representación legal e institucional.
- c) Aprobar las Circulares de la Agencia Española de Protección de Datos, de conformidad con lo previsto en el artículo 6 del presente Estatuto.
- d) Dictar las resoluciones y directrices que requiera el ejercicio de las funciones de la Agencia, en particular las derivadas del ejercicio de las competencias previstas en el artículo 57 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y del ejercicio de los poderes de investigación y de los poderes correctivos dispuestos en el artículo 58 del citado Reglamento.
- e) Acordar la realización de planes de auditoría preventiva y dictar las directrices generales o específicas que resulten de las mismas.
- f) Convocar, por iniciativa propia o cuando lo solicite otra autoridad y, en todo caso, cada seis meses, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre.
- g) Solicitar y facilitar a las autoridades autonómicas de protección de datos la información necesaria para el cumplimiento de sus funciones, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos.
- h) Requerir a las autoridades autonómicas de protección de datos cuando considere que un tratamiento llevado a cabo en materias que fueran competencia de aquellas vulnera el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, para que adopten las medidas necesarias para su cesación y ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.
- i) Participar en las actividades y reuniones del Comité europeo de protección de datos como representante común del Estado español.
- j) Ejercer todas aquellas funciones no atribuidas expresamente a otros órganos de la Agencia Española de Protección de Datos.

2. Asimismo, le corresponde:

- a) Llevar a cabo la dirección y gestión ordinaria de la Agencia, en el marco de las funciones atribuidas en este apartado.
- b) Informar al Consejo Consultivo de cuantos asuntos conciernan a los servicios a su cargo.
- c) Ser órgano de contratación de la entidad.
- d) Formular y aprobar las cuentas anuales de la entidad, junto con el informe de auditoría de cuentas, de conformidad con lo dispuesto en la Ley 47/2003, de 26 de noviembre, General Presupuestaria.
- e) Acordar las variaciones presupuestarias que se estimen necesarias y que no deban ser autorizadas por la persona titular del Ministerio de Hacienda y proponer aquellas que precisan autorización.
- f) Autorizar, por causa justificada, la disposición de gastos, el reconocimiento de obligaciones y ordenar los pagos correspondientes y movimientos de fondos.
- g) Proponer la modificación de los límites generales de compromiso de gasto con cargo a ejercicios futuros por causa justificada.
- h) Suscribir, en el ámbito de sus competencias, convenios con entidades públicas y privadas.
- i) Ejercer la jefatura superior del personal y prever las necesidades de personal de la Agencia Española de Protección de Datos a incorporar en la oferta anual de empleo público, en los términos previstos en el artículo 32, aprobar las relaciones de puestos de trabajo en el marco de los criterios establecidos por el Ministerio de Hacienda y la distribución del complemento de productividad y otros incentivos al rendimiento, dentro de la cantidad autorizada a estos efectos.
- j) Convocar y resolver los procesos de provisión de puestos de trabajo que integren al personal de la Agencia Española de Protección de Datos y contratar al personal laboral a su servicio en los términos previstos en el artículo 34.
- k) Acordar las actuaciones en materia de gestión patrimonial de la entidad.
- l) La aprobación del inventario de bienes y derechos de conformidad con lo establecido en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- m) Las demás facultades que le atribuya el Estatuto.

Artículo 14. Independencia.

1. La persona titular de la Presidencia de la Agencia Española de Protección de Datos desempeñará su cargo con dedicación exclusiva, plena independencia y total objetividad.
2. La persona titular de la Presidencia no recibirá instrucciones de autoridad alguna.

Artículo 15. Delegación de competencias.

La Presidencia de la Agencia podrá delegar sus funciones en la Adjuntía a la Presidencia, así como en las Subdirecciones Generales que dependan directamente de la Presidencia y en la Secretaría General, en los términos previstos en el artículo 9 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

En ningún caso podrán ser objeto de delegación las funciones relacionadas con los procedimientos regulados por el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, de conformidad con el artículo 48.2. de la misma, ni la facultad para aprobar los proyectos de circulares, de acuerdo con el artículo 6.9 del presente Estatuto.

Sección 2.ª La Adjuntía a la Presidencia de la Agencia Española de Protección de Datos

Artículo 16. Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.

1. La persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos tendrá la consideración de alto cargo, con rango de Director General.
2. La persona titular de la Adjuntía a la Presidencia será designado de conformidad con el procedimiento establecido en el artículo 48 de la Ley Orgánica 3/2018, de 5 de diciembre, y solo cesará por las causas que en el mismo se establecen.

3. La persona titular de la Adjuntía a la Presidencia poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

4. La persona titular de la Adjuntía a la Presidencia cesante continuará en funciones hasta la toma de posesión del nuevo titular.

5. La Adjuntía a la Presidencia es un cargo de dedicación exclusiva, está sujeto al régimen de incompatibilidades de los altos cargos de la Administración General del Estado, y será incompatible con el ejercicio de cualquier actividad pública o privada, retribuida o no, salvo las que sean inherentes a su condición de Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.

Artículo 17. *Funciones de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos.*

Corresponderán a la persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos las siguientes competencias:

a) Ejercer las funciones de la Presidencia de la Agencia Española de Protección de Datos en los casos de delegación previstos en la Ley Orgánica 3/2018, de 5 de diciembre, y en este Estatuto. A estos efectos, la Presidencia podrá delegar sus funciones en la Adjuntía a la Presidencia, a excepción de las relacionadas con los procedimientos regulados en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre.

b) Colaborar con la Presidencia de la Agencia Española de Protección de Datos en las relaciones con las Cortes Generales y con el Defensor del Pueblo y en la cooperación con las autoridades de control de las Comunidades Autónomas.

c) Colaborar con la Presidencia de la Agencia Española de Protección de Datos en la planificación y desarrollo de la actividad internacional de la Agencia.

d) Impulsar el procedimiento de elaboración de circulares de conformidad con lo previsto en el artículo 6 del presente Estatuto.

e) Preparar y proponer a la Presidencia de la Agencia Española de Protección de Datos el borrador del Plan estratégico y de la Memoria anual, así como el impulso y seguimiento de las actuaciones una vez aprobadas.

f) Coordinar la formación especializada de la Agencia.

g) Asumir las restantes funciones que se le encomiendan en las leyes y disposiciones reglamentarias vigentes.

Artículo 18. *Independencia.*

1. La persona titular de la Adjuntía a la Presidencia de la Agencia Española de Protección de Datos desempeñará su cargo con dedicación exclusiva, plena independencia y total objetividad.

2. Sin perjuicio de las competencias que corresponden a la Presidencia de la Agencia Española de Protección de Datos, la persona titular de la Adjuntía no recibirá instrucciones de autoridad alguna.

Sección 3.^a Procedimiento de designación de la Presidencia y la Adjuntía

Artículo 19. *Inicio del procedimiento de nombramiento y convocatoria.*

1. Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, se publicará en el «Boletín Oficial del Estado» la convocatoria pública de personas candidatas mediante orden de la persona titular del Ministerio de Justicia.

2. En la orden se regularán las bases de la convocatoria.

En ella se especificarán los requisitos a evaluar de las personas candidatas, que permitan acreditar que se trata de personas de reconocida competencia profesional, en particular en materia de protección de datos, sobre la base del mérito, la capacidad, la competencia y la idoneidad, entre los que se pueden recoger las capacidades legales de la persona candidata, la experiencia profesional, la capacidad de desarrollar el trabajo o los conocimientos técnicos, en particular referidos al ámbito de protección de datos.

3. La idoneidad de las personas candidatas exigirá que su independencia, conducta intachable e integridad deben estar fuera de toda duda.

4. Las solicitudes de participación en el procedimiento de selección se presentarán en cualquiera de los lugares previstos en el artículo 16.4 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 20. *Comité de selección.*

1. Una vez convocado el procedimiento, se constituirá un comité de selección con la finalidad de examinar las candidaturas y proponer la persona candidata más idónea.

2. El comité estará compuesto por:

- a) La persona titular de la Secretaría de Estado de Justicia, que ostentará la Presidencia.
- b) La persona titular de la Subsecretaría del Ministerio para la Presidencia, Relaciones con las Cortes y Memoria Democrática.
- c) Un Magistrado o una Magistrada de la Sala Tercera del Tribunal Supremo, a propuesta del Ministerio de Justicia.
- d) Un o una jurista de reconocida competencia, con al menos diez años de actividad profesional en materia de protección de datos, a propuesta del Ministerio de Justicia.
- e) La persona titular de un organismo de protección de datos autonómico o una de las personas que hayan ocupado el puesto de la Dirección o Presidencia de la Agencia Española de Protección de Datos con anterioridad al saliente, a propuesta del Ministerio de Justicia.

3. La Secretaría corresponderá a un miembro de la Abogacía del Estado, designado por la persona titular de la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, que asistirá a las reuniones con voz, pero sin voto.

Los acuerdos del comité de selección se adoptarán por mayoría de sus miembros.

4. El comité de selección deberá ser paritario.

5. Podrá recabar el apoyo de las personas asesoras que estime necesarias para la correcta realización de sus funciones.

Artículo 21. *Principios aplicables al procedimiento.*

El procedimiento respetará en todas sus fases los principios de mérito, capacidad, competencia e idoneidad, así como el principio de igualdad de trato entre mujeres y hombres en el acceso al empleo público, de acuerdo con la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, y el principio de igualdad en el acceso a las funciones y cargos públicos recogido en el artículo 23.2 de la Constitución. La convocatoria respetará también los principios de igualdad y no discriminación de las personas con discapacidad.

Artículo 22. *Propuesta y comunicación de candidaturas.*

1. El comité de selección examinará las solicitudes junto con la documentación aportada y realizará, en su caso, las entrevistas oportunas.

2. Una vez valoradas las solicitudes de participación en el procedimiento de selección, el comité de selección propondrá una candidatura la Presidencia de la Agencia Española de Protección de Datos y a la Adjuntía a la Presidencia de entre aquellas que cumplan los requisitos establecidos en los artículos 12.2 y 16.3, respectivamente y atendidos los méritos y criterios de valoración establecidos en la convocatoria, junto con su informe justificativo.

La persona titular del Ministerio de Justicia elevará dicha propuesta junto con el informe del comité de selección al Consejo de Ministros.

3. El Consejo de Ministros debatirá la propuesta del comité de selección a la luz del informe y decidirá mediante acuerdo la propuesta de Presidencia y Adjuntía, que se remitirá al Congreso de los Diputados acompañada del informe justificativo.

En caso de que el Consejo de Ministros considere que la propuesta realizada por el comité de selección no resulta idónea la devolverá al comité de selección mediante acuerdo motivado, otorgándole un nuevo plazo para que formule nueva propuesta al Consejo de Ministros.

4. El acuerdo adoptado en el Consejo de Ministros con la propuesta de Presidencia y Adjuntía será publicado en el «Boletín Oficial del Estado» mediante orden de la persona titular del Ministerio de Justicia.

Sección 4.ª El Consejo Consultivo de la Agencia Española de Protección de Datos

Artículo 23. El Consejo Consultivo.

1. El Consejo Consultivo de la Agencia Española de Protección de Datos, con la composición que se establece en el artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre, es un órgano colegiado de asesoramiento de la Presidencia de la Agencia Española de Protección de Datos.

2. El Consejo Consultivo emitirá informe en todas las cuestiones que le someta la Presidencia de la Agencia de Protección de Datos y podrá formular propuestas en temas relacionados con las materias de competencia de esta.

Artículo 24. Plazo y vacantes.

1. Los miembros del Consejo Consultivo desempeñarán su cargo durante cinco años.
2. Se exceptúan de lo establecido en el apartado anterior los siguientes supuestos:

a) Nombramiento del Vocal para desempeñar la Presidencia de la Agencia de Protección de Datos o la Adjuntía a la Presidencia.

b) Renuncia anticipada del Vocal.

c) Pérdida de la condición que habilitó al Vocal para ser propuesto, en los supuestos previstos en las letras a) y b) del artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre.

d) Propuesta de cese emanada de las instituciones, órganos, corporaciones u organizaciones a las que se refiere el citado artículo.

3. Las vacantes que se produzcan en el Consejo Consultivo antes de expirar el plazo a que se refiere el apartado 1 deberán ser cubiertas dentro del mes siguiente a la fecha en que la vacante se hubiera producido, en la forma establecida por el artículo 49.3 de la Ley Orgánica 3/2018, de 5 de diciembre, y por el tiempo que reste para completar el mandato de quien causó la vacante a cubrir.

4. Los miembros del Consejo Consultivo no percibirán retribución alguna, sin perjuicio del abono de los gastos, debidamente justificados, que les ocasione el ejercicio de su función de conformidad, en su caso, con lo establecido en el Real Decreto 462/2002, de 24 de mayo, sobre indemnizaciones por razón del servicio.

Artículo 25. Renovación del Consejo Consultivo.

1. Antes de finalizar el mandato de los miembros del Consejo Consultivo, la persona titular del Ministerio de Justicia requerirá a las instituciones, órganos, corporaciones y organizaciones a que se refiere el artículo 49 de la Ley Orgánica 3/2018, de 5 de diciembre, a fin de que le comuniquen los nombres de las personas que propongan para un nuevo mandato en el Consejo Consultivo, lo que deberá efectuarse dentro del mes siguiente a la formulación del referido requerimiento.

2. Una vez transcurrido el plazo señalado para cumplimentar el requerimiento, la persona titular del Ministerio de Justicia procederá, sin más trámites, a nombrar como miembros del Consejo Consultivo, mediante Orden que se publicará en el «Boletín Oficial del Estado», a los propuestos, quienes tomarán posesión de su condición en la misma fecha en que expire el mandato de los miembros del Consejo anterior.

Artículo 26. Funcionamiento.

1. En lo no previsto en la Ley Orgánica 3/2018, de 5 de diciembre, y en el presente Estatuto, el Consejo Consultivo se regirá por lo establecido en materia de órganos colegiados por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Consejo Consultivo adoptará sus acuerdos en sesión plenaria.

3. Actuará como Presidencia del Consejo Consultivo la Presidencia de la Agencia de Protección de Datos.

4. Desempeñará la Secretaría del Consejo Consultivo, con voz y sin voto, el titular de la Secretaría General de la Agencia de Protección de Datos. En caso de vacante, ausencia o enfermedad, desempeñará la Secretaría una persona funcionaria adscrita a la Secretaría General designado por la Presidencia de la Agencia a tal efecto.

5. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia y, en todo caso, una vez al semestre. También se reunirá cuando así lo solicite la mayoría de sus miembros.

6. La persona que desempeñe la Secretaría convocará las reuniones del Consejo Consultivo, de orden de la Presidencia de la Agencia, y trasladará la convocatoria a los miembros del Consejo.

7. El Consejo Consultivo quedará válidamente constituido, en primera convocatoria, si están presentes la persona que actúe como Presidencia, la persona que desempeñe la Secretaría y la mitad de los miembros del Consejo, y, en segunda convocatoria, si están presentes la persona que actúe como Presidencia, la persona que desempeñe la Secretaría y la tercera parte de los miembros del Consejo.

8. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

Sección 5.ª Otros órganos directamente dependientes de la Presidencia de la Agencia Española de Protección de Datos

Artículo 27. *La Subdirección General de Inspección de Datos.*

1. La Subdirección General de Inspección de Datos es el órgano administrativo, dependiente de la Presidencia de la Agencia Española de Protección de Datos, que desarrolla las competencias previstas en el artículo 57.1, letras f), g), h), i) y u) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y realiza las funciones de inspección y de instrucción necesarias para el ejercicio de los poderes de investigación establecidos en el artículo 58.1, letras a), b), d), e) y f) y de los poderes correctivos dispuestos en el artículo 58.2, letras a), b), c), d), f), g), i) y j), ambos del citado Reglamento.

2. Al objeto de cumplir los cometidos establecidos en el apartado anterior, a la Subdirección General de Inspección de Datos le corresponden las siguientes funciones:

a) La supervisión permanente del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las disposiciones que la desarrollen, por parte de los responsables y encargados de los tratamientos.

b) El ejercicio de las potestades de investigación definidas en el artículo 51 de la Ley Orgánica 3/2018, de 5 de diciembre.

c) La realización de planes de auditoría preventiva que contempla el artículo 54 de la Ley Orgánica 3/2018, de 5 de diciembre, referidos a los tratamientos de un sector concreto de actividad. A resultados de esos planes, le corresponde la propuesta a la Presidencia de la Agencia de emisión de directrices generales o específicas tendentes a asegurar la plena adaptación del sector o responsable a la normativa y a procurar la aplicación de los derechos y garantías reconocidos en el título X de la Ley Orgánica 3/2018, de 5 de diciembre, en la medida en que estos afecten a tratamientos de datos personales cuya investigación, y en su caso, propuesta de imposición de medida correctiva o sancionadora, corresponda a la Subdirección General de Inspección de Datos.

d) La tramitación de los procedimientos en caso de posible vulneración de la normativa de protección de datos conforme a lo dispuesto en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, incluyendo las reclamaciones de los ciudadanos por falta de atención en sus solicitudes de ejercicio de los derechos contemplados en los artículos 15 al 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Corresponde a la Subdirección General de Inspección de Datos el deber de informar al reclamante sobre el curso y el resultado de la reclamación presentada ante la Agencia

Española de Protección de Datos, de acuerdo con lo dispuesto en el artículo 77.2 del citado Reglamento.

e) La evaluación de la admisibilidad a trámite de las reclamaciones que se presenten ante la Agencia Española de Protección de Datos, y la propuesta a la Presidencia de decisión sobre la admisión o inadmisión a trámite, conforme a lo establecido en el artículo 65 de la Ley Orgánica 3/2018, de 5 de diciembre.

f) El traslado de la reclamación al responsable del tratamiento o a su Delegado de Protección de Datos, o al organismo de supervisión establecido para la aplicación de los códigos de conducta, a fin de que den respuesta a la reclamación antes de resolver sobre su admisión a trámite, según lo establecido en el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre.

g) El análisis de la competencia de la Agencia Española de Protección de Datos respecto de las reclamaciones que reciba, la determinación de su carácter nacional o transfronterizo, y la remisión, cuando proceda, a la autoridad de control principal que se determine, según lo dispuesto en el artículo 66 de la Ley Orgánica 3/2018, de 5 de diciembre.

h) La realización de actuaciones previas de investigación acordadas por la Presidencia por propia iniciativa, a raíz de una reclamación, o a petición de otro órgano o autoridad de control, a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento, según lo dispuesto en el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre.

i) La instrucción del procedimiento para el ejercicio de la potestad sancionadora en caso de infracción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las normas de derecho interno que la desarrollen, conforme al régimen sancionador dispuesto en el título IX de la citada ley orgánica.

j) La propuesta a la Presidencia del acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora, según lo establecido en el artículo 68 de la Ley Orgánica 3/2018, de 5 de diciembre.

k) Durante las actuaciones previas de investigación o iniciado un procedimiento sancionador, la propuesta a la Presidencia de acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos, y en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado, conforme a lo establecido en el artículo 69 de la Ley Orgánica 3/2018, de 5 de diciembre.

l) La instrucción del procedimiento para el ejercicio de la potestad sancionadora por la comisión de las infracciones tipificadas en los artículos 38.3.c), d) e i) y 38.4.d), g) y h) de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, conforme a lo dispuesto en el artículo 43.1 de la citada Ley.

m) La instrucción del procedimiento para el ejercicio de la potestad sancionadora por la comisión de las infracciones graves del artículo 77 tipificadas en el apartado 37 y de las infracciones leves del artículo 78 tipificadas en el apartado 11 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, cuando se vulneren los derechos de los usuarios finales sobre protección de datos y privacidad reconocidos en el artículo 48, de acuerdo con lo establecido en el artículo 84.3 de la referida Ley.

n) La propuesta a la Presidencia de la Agencia de imponer aquella medida correctiva que resulte idónea en cada caso para garantizar la protección de los datos de carácter personal. Conforme a lo dispuesto en el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, podrá proponer que se ordene al responsable o encargado del tratamiento que atienda las solicitudes de ejercicio de los derechos del interesado, ordenar al responsable o encargado que las operaciones de tratamiento se ajusten a la normativa o se realicen de una determinada manera y dentro de un plazo especificado, que se imponga una limitación temporal o definitiva del tratamiento, incluida su prohibición o que se ordene la suspensión de flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

o) En la instrucción de los procedimientos sancionadores, de acuerdo con lo previsto en el artículo 76 de la Ley Orgánica 3/2018, de 5 de diciembre, la propuesta a la Presidencia de

imponer la sanción que se considere adecuada, que podrá ser de multa administrativa además o en lugar de las otras medidas correctivas previstas en el artículo 58.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, atendiendo a los hechos y a las circunstancias de cada caso individual y a las condiciones establecidas en el artículo 83 del citado Reglamento.

p) Respecto de las reclamaciones que gestiona, de las actuaciones de investigación que realiza y de los procedimientos sancionadores que instruye, la práctica de las notificaciones y comunicaciones que sean precisas en los actos de trámite, así como el registro de los datos pertinentes en el sistema de comunicación con las autoridades de control de la Unión Europea.

q) La gestión de registros internos de infracciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y de las medidas adoptadas, según lo establecido en el artículo 57.1 u) del citado Reglamento.

r) La cooperación con las autoridades autonómicas de protección de datos que hubiesen asumido el ejercicio de las funciones establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, remitiéndoles aquellas reclamaciones que sean de su competencia conforme a lo dispuesto en el artículo 57 de la Ley Orgánica 3/2018, de 5 de diciembre.

s) La participación en la acción exterior de la Agencia Española de Protección de Datos en lo referente a las competencias de la Subdirección General. Particularmente, la cooperación con las demás autoridades de control de la Unión Europea respecto de las reclamaciones por infracción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de las actuaciones de investigación y de los procedimientos sancionadores que tramiten las autoridades de control de los Estados miembros, compartiendo información y prestando asistencia mutua, conforme a lo establecido en sus artículos 59, 60 y 61 del citado Reglamento, con el fin de garantizar la coherencia en la aplicación y ejecución del mismo.

t) Respecto de los recursos que se interpongan contra las actuaciones realizadas por la Subdirección General, la tramitación de los recursos en vía administrativa, así como la coordinación de la relación con los órganos jurisdiccionales y con los demás órganos de la Agencia que intervienen en la gestión de los recursos contencioso-administrativos.

u) La coordinación de la aplicación, en el ámbito de la Subdirección General, del sistema informático que establezca el Comité Europeo de Protección de Datos para la comunicación y compartición de la información entre las autoridades de protección de datos de la Unión Europea.

Artículo 28. *La Subdirección General de Promoción y Autorizaciones.*

Corresponde a la Subdirección General de Promoción y Autorizaciones el desarrollo de las siguientes funciones:

a) Promover la sensibilización de la ciudadanía y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de datos, en especial cuando se trate de actividades dirigidas específicamente a los niños, según lo establecido en el artículo 57.1.b del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

b) Promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, según lo dispuesto en su artículo 57.1.d.

c) Facilitar, previa solicitud, información a los ciudadanos en relación con el ejercicio de sus derechos en virtud del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conforme a su artículo 57.1.e.

d) El registro y publicidad de los delegados de protección de datos de acuerdo con los artículos 37.7 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 34.4 de la Ley Orgánica 3/2018, de 5 de diciembre.

e) Elaborar las cláusulas contractuales tipo a que se refieren el artículo 28.8 y el artículo 46.2.d del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril

de 2016, y proponer a la Presidencia su aprobación o adopción, de acuerdo con su artículo 57.1.j).

f) Alentar la elaboración de códigos de conducta y dictaminar y proponer a la Presidencia la aprobación de los que proporcionen suficientes garantías con arreglo al artículo 40.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conforme a su artículo 57.1 m).

g) Elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de acuerdo con su artículo 57.1.p).

h) Proponer a la Presidencia la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en virtud de su artículo 57.1.q).

i) Fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos según lo previsto en el artículo 57.1.n) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, proponer a la Presidencia la aprobación de los criterios de certificación de conformidad con el artículo 42.5 del mismo y la expedición de certificaciones; el registro de las concesiones, denegaciones o revocaciones de las acreditaciones y de las certificaciones expedidas y la realización de revisiones periódicas de las certificaciones expedidas, conforme a los artículos 43.5 y 57.1.n) y o) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y el artículo 39 de la Ley Orgánica 3/2018, de 5 de diciembre.

j) Proponer a la Presidencia la retirada de certificaciones o la orden al organismo de certificación para que retire certificaciones emitidas con arreglo a los artículos 42 y 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, o que no se emita una certificación cuando no se cumplan o dejen de cumplirse los requisitos para la certificación, de acuerdo con el artículo 58.2.h) del mismo.

k) Proponer a la Presidencia la autorización de las transferencias internacionales en virtud de cláusulas contractuales y acuerdos administrativos a que se refiere el artículo 46, apartado 3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, de acuerdo con su artículo. 57.1.r).

l) Proponer a la Presidencia la aprobación de normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en su artículo 57.1.s).

m) Proponer a la Presidencia la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional de acuerdo con el artículo 58.2 j) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en los supuestos de modificación de las circunstancias que determinaron el otorgamiento de la autorización o la aprobación a que se refieren los dos apartados anteriores.

n) El registro de los sistemas de exclusión publicitaria y su publicación conforme a lo dispuesto en el artículo 23.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

o) Proponer a la Presidencia las excepciones a la obligación de bloqueo en los supuestos establecidos en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

p) El ejercicio de las funciones que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno, atribuye a las Unidades de Información.

q) La gestión de las quejas y sugerencias, de conformidad con el Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

Artículo 29. *La Secretaría General de la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos contará con una Secretaría General, con nivel orgánico de subdirección general, bajo la inmediata dirección de la Presidencia, a la que corresponde tener a su cargo los servicios comunes y de carácter administrativo de la entidad.

2. La Secretaría General de la Agencia Española de Protección de Datos tendrá atribuidas las siguientes funciones:

- a) Elaborar los informes y propuestas que le solicite la Presidencia.
- b) Notificar las resoluciones de la Presidencia, salvo las que se dicten por delegación, que se notificarán por el órgano delegado.
- c) Ejercer la Secretaría del Consejo Consultivo: Preparar los asuntos y documentación que hayan de someterse a las deliberaciones del mismo, levantar las actas de las sesiones, expedir certificaciones de los acuerdos adoptados y tramitar los acuerdos adoptados.
- d) La colaboración en la preparación de conferencias, seminarios y cualesquiera otras actividades similares que organice la Agencia Española de Protección de Datos.
- e) La gestión y administración de recursos humanos incluida la elaboración de la relación de puestos de trabajo, la gestión de los procesos de selección del personal laboral, la gestión de la acción social y la formación de los recursos humanos, bajo la supervisión de la Presidencia.
- f) La planificación y ejecución de la política de prevención de riesgos laborales.
- g) El mantenimiento de las relaciones con los órganos de participación y representación del personal.
- h) La gestión de los recursos materiales de la Agencia Española de Protección de Datos, y en el ejercicio de las competencias en materia patrimonial correspondientes a la Agencia, la conservación y mantenimiento y seguridad de su patrimonio y llevar el inventario de los bienes y derechos que se integren en él.
- i) El régimen interior, asuntos generales y la coordinación e inspección de las instalaciones y servicios de la Agencia.
- j) La gestión económico-financiera y patrimonial de la entidad, la elaboración del anteproyecto del presupuesto anual de la Agencia Española de Protección de Datos y la tramitación de sus variaciones.
- k) La tramitación de los expedientes de contratación para adquisición de bienes y servicios, así como la habilitación del material.
- l) La gestión presupuestaria, de los ingresos y gastos, la realización de los cobros y pagos y la gestión de la tesorería de la Agencia.
- m) Las actuaciones referentes a la gestión contable y su tramitación documental, y a la preparación de las cuentas de la entidad para su rendición y aprobación.
- n) Organizar, supervisar, liquidar y controlar la recaudación en periodo voluntario de los ingresos por sanciones impuestas por la Agencia Española de Protección de Datos al amparo de lo previsto por el artículo 46 de la Ley Orgánica 3/2018, de 5 de diciembre.
- o) La dirección y organización de los servicios de archivo y registro de la Agencia Española de Protección de Datos.
- p) El desarrollo de los sistemas de información de los servicios comunes, de los sistemas de administración electrónica, el diseño y ejecución de planes y coordinación de las actuaciones y prestación de los servicios en materia de tecnologías de la información y comunicaciones, la gestión y mantenimiento de la sede electrónica y de los sitios web, la gestión de la red interna de comunicaciones, la gestión de los medios informáticos y telemáticos y su asignación a las distintas unidades orgánicas.
En el ejercicio de estas funciones, la Secretaría General podrá optar por la utilización y el aprovechamiento de módulos y servicios comunes de administración electrónica, en los términos que se acuerden con los órganos responsables en esta materia de la Administración General del Estado.
- q) Redactar, proponer y tramitar los convenios con entidades públicas y privadas a celebrar por la Presidencia de la Agencia Española de Protección de Datos.
- r) El ejercicio de las competencias en materia de gestión documental, estadística, recursos documentales, biblioteca y publicaciones de la Agencia Española de Protección de Datos.
- s) El diseño e implementación de un sistema de evaluación del desempeño del personal en el marco de lo establecido en la normativa vigente.
- t) Ejercer las potestades administrativas derivadas de las funciones de la Agencia, así como la gestión de los asuntos horizontales que no se correspondan con competencias

específicamente atribuidas a otras unidades de la Agencia y las que le sean atribuidas por normas legales o reglamentarias.

u) Desempeñar las demás facultades y funciones que le atribuya el Estatuto y cualesquiera otras normas aplicables, así como las que le deleguen, en su caso, la Presidencia, de entre las contempladas en las letras a) a l) del apartado 2 del artículo 13.

Artículo 30. *División de Relaciones Internacionales.*

Corresponde a la División de Relaciones Internacionales:

a) Organizar y coordinar la actividad internacional de la Agencia Española de Protección de Datos en su ámbito competencial, de acuerdo con los criterios y directrices establecidos por la Presidencia de la Agencia.

b) Coordinar la participación de la Agencia Española de Protección de Datos en reuniones, organizaciones y foros internacionales, en particular en el ámbito del Comité Europeo de Protección de Datos o en otros grupos de trabajo en materia de protección de datos constituidos al amparo del Derecho de la Unión Europea.

c) Coordinar la preparación de la posición de la Agencia Española de Protección de Datos en las discusiones y negociaciones internacionales, en particular en las desarrolladas en el seno del Comité Europeo de Protección de Datos.

d) Coordinar y asesorar a los órganos de la Agencia Española de Protección de Datos de los aspectos internacionales relacionados con sus funciones, en particular los que se deriven de la actividad del Comité Europeo de Protección de Datos.

e) Elaborar informes, estudios o análisis sobre la situación o evolución en el ámbito internacional de las materias relacionadas con la protección de datos.

f) Contribuir, sin perjuicio de la competencia específica de otros órganos de la Agencia y conforme a las directrices de la Presidencia, a la coordinación de la cooperación en la acción exterior en materias relacionadas con la protección de datos con otros órganos de la Administración General del Estado y entidades del sector público estatal, así como de las comunidades autónomas, y con las entidades locales, en particular con las autoridades autonómicas de protección de datos.

g) Organizar y coordinar la participación de la Agencia Española de Protección de Datos en proyectos y actividades de carácter internacional en materia de protección de datos.

Artículo 31. *División de Innovación Tecnológica.*

Corresponde a la División de Innovación Tecnológica:

a) Asesorar a la Presidencia de la Agencia Española de Protección de Datos, como a sus distintas unidades, sobre los temas tecnológicos que tienen relevancia en la protección de datos de carácter personal, y para ello, analizar las implicaciones y alternativas del estado de arte de la tecnología y generar el conocimiento necesario para anticiparse a los cambios de la misma.

b) Impulsar la protección de datos como un factor de confianza y garantía de calidad en beneficio del desarrollo económico de la sociedad con el objeto de promover la sensibilización de responsables y ciudadanos, incluido el desarrollo y mantenimiento de herramientas de ayuda para el cumplimiento por parte de los mismos y la elaboración de guías que impulsen el cumplimiento del principio de responsabilidad activa del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el ámbito tecnológico, según su artículo 57.1.b) y d).

c) Impulsar las medidas que garanticen la compatibilidad del desarrollo tecnológico con la privacidad asegurando los derechos de los ciudadanos según lo previsto en el artículo 57.1.i) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; en particular: el asesoramiento a emprendedores y desarrolladores tecnológicos, la realización de estudios de prospección tecnológica, informar y asesorar a los proyectos tecnológicos con implicaciones en el derecho a la protección de datos de las personas, participar en proyectos tecnológicos de ámbito internacional de interés público sobre la base del derecho de la Unión Europea o de los Estados Miembros y promover la colaboración con las Universidades con el fin de impulsar la protección de datos en proyectos y contenidos curriculares jurídicos y técnicos.

d) Gestionar el Registro de brechas de seguridad para facilitar a los responsables el cumplimiento de lo previsto en el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

e) Analizar y clasificar las brechas de seguridad y, en su caso, proponer motivadamente a la Presidencia la iniciación de una investigación cuando aprecie indicios de la comisión de una infracción.

f) Emitir informes, recomendaciones y dictámenes sobre las consultas previas realizadas por los responsables conforme al artículo 36 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en virtud de lo previsto en su artículo 57.1.i).

g) Elaborar una lista positiva y, en su caso, otra negativa de tratamientos que requieren la realización de evaluaciones de impacto según lo previsto en el artículo 57.1.k) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

CAPÍTULO III

Personal al servicio de la Agencia Española de Protección de Datos

Artículo 32. Régimen de Personal.

1. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral.

2. En todo caso, el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas o en la salvaguardia de los intereses generales del Estado y de las Administraciones Públicas, corresponden exclusivamente al personal funcionario público.

3. La persona titular de la Presidencia de la Agencia Española de Protección de Datos presentará anualmente al Ministerio de Política Territorial y Función Pública la propuesta de oferta de empleo público de la Agencia, para su aprobación e inclusión independiente en la oferta de empleo público de la Administración General del Estado. Dicha propuesta tendrá en cuenta las necesidades de recursos humanos de la Agencia para el adecuado ejercicio de sus funciones.

Artículo 33. Personal funcionario.

1. El personal funcionario de la Agencia Española de Protección de Datos se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normas aplicables al personal funcionario de la Administración General del Estado.

2. El personal funcionario que desarrolle actividades de investigación tendrá la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

3. La Presidencia de la Agencia Española de Protección de Datos convocará y resolverá los procedimientos de provisión de puestos de trabajo de conformidad con los procedimientos de provisión establecidos en la normativa sobre función pública. Tanto las convocatorias como sus resoluciones se publicarán en el «Boletín Oficial del Estado».

Artículo 34. Personal laboral.

1. El personal laboral de la Agencia Española de Protección de Datos se regirá por el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, la normativa convencional aplicable en su caso, y por los preceptos del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, que expresamente le resulten de aplicación.

2. Corresponderá a la Presidencia de la Agencia Española de Protección de Datos la celebración de los contratos de trabajo del personal laboral, que será seleccionado, en ejecución de la Oferta de Empleo Público prevista en el artículo 32, mediante convocatoria pública que, además de adecuarse a la relación de puestos de trabajo de la Agencia, se

sujetará a los principios de igualdad, mérito, capacidad y publicidad previstos por el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, así como del acceso al empleo público de las personas con discapacidad.

Artículo 35. *Relación de puestos de trabajo.*

1. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por los Ministerios de Hacienda y de Política Territorial y Función Pública, respetando el límite de gasto de personal establecido en el presupuesto.

2. Las relaciones de puestos de trabajo de la Agencia Española de Protección de Datos comprenderán de forma diferenciada:

a) Los puestos de trabajo a desempeñar por personal funcionario; y contendrá su denominación, tipo y sistema de provisión, requisitos exigidos para su desempeño; así como el nivel de destino, y, en su caso, el complemento específico que corresponden a los mismos.

b) Los puestos de trabajo a desempeñar por personal laboral, fijo o temporal, contendrá el grupo profesional, familia profesional y/o especialidad y complementos del puesto; así como las características específicas del mismo, cuando proceda, y, en su caso, los requisitos de carácter profesional necesarios para su desempeño.

Artículo 36. *Retribuciones.*

Las retribuciones del personal funcionario y laboral de la Agencia se ajustarán de acuerdo con lo dispuesto en la materia en las leyes de Presupuestos Generales del Estado.

Artículo 37. *Evaluación del desempeño.*

En el marco de la política de recursos humanos, y conforme a los principios establecidos en el Real Decreto Legislativo 5/2015, de 30 de octubre, se establecerá un sistema de evaluación que sirva de instrumento objetivo para la valoración del desempeño del puesto de trabajo, a efectos retributivos y de carrera profesional del personal al servicio de la entidad. El correspondiente sistema de evaluación permitirá valorar los rendimientos colectivos de las unidades, así como realizar una valoración individual del desempeño de cada puesto de trabajo.

Artículo 38. *Incompatibilidades del personal de la Agencia Española de Protección de Datos.*

El personal de la Agencia Española de Protección de Datos estará sujeto a la Ley 53/1984, de 26 de diciembre, de Incompatibilidades del Personal al Servicio de las Administraciones Públicas.

Artículo 39. *Deber de secreto profesional.*

El personal al servicio de la Agencia Española de Protección de Datos deberá guardar secreto, incluso después de cesar en sus funciones, sobre los datos personales que conozcan en el desempeño de sus tareas y de cuantas informaciones de naturaleza confidencial hubiera conocido en el ejercicio de aquellas.

A tal efecto, la Agencia Española de Protección de Datos elaborará una política específica para garantizar la confidencialidad de la información que no tenga el carácter de pública, dentro de la cual se integrará el Código Ético del personal al servicio de la Agencia, que será objeto de publicación en su página web.

CAPÍTULO IV

Régimen económico, presupuestario, patrimonial y de contratación

Sección 1.ª Régimen económico-financiero, patrimonial y de contratación

Artículo 40. *Recursos económicos.*

1. Los recursos económicos de la Agencia Española de Protección de Datos comprenderán:

a) Las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyen su patrimonio y los productos y rentas de dicho patrimonio.

c) Los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidas en el artículo 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

d) Las subvenciones y aportaciones que se concedan a su favor, procedentes de fondos específicos de la Unión Europea o de otros organismos internacionales.

e) Cualesquiera otros que legalmente puedan serle atribuidos.

2. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

Artículo 41. *Recaudación.*

1. La gestión y recaudación de las tasas, precios públicos y cualesquiera otros recursos públicos cuya gestión esté atribuida a la Agencia Española de Protección de Datos, corresponde a dicha Autoridad, pudiendo utilizar para la efectividad de los mismos el procedimiento administrativo de apremio.

2. La Agencia Española de Protección de Datos podrá convenir con la Agencia Estatal de Administración Tributaria la gestión recaudatoria en período ejecutivo de sus recursos de derecho público en la forma prevista en el Reglamento General de Recaudación aprobado por Real Decreto 939/2005, de 29 de julio.

Artículo 42. *Patrimonio.*

1. La Agencia Española de Protección de Datos tendrá, para el cumplimiento de sus fines, un patrimonio propio e independiente del de la Administración General del Estado, integrado por el conjunto de bienes y derechos de los que sea titular.

2. La gestión y administración de los bienes y derechos propios, así como de aquellos del Patrimonio del Estado que se le adscriban para el cumplimiento de sus fines, será ejercida de acuerdo con lo señalado en este Estatuto y con lo establecido para los organismos públicos en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

3. Corresponde a la Presidencia de la Agencia Española de Protección de Datos acordar la adquisición por cualquier título de los bienes inmuebles y derechos que resulten necesarios para los fines de la institución, así como su uso y arrendamiento, de acuerdo con el procedimiento establecido en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

4. La Agencia Española de Protección de Datos formará y mantendrá actualizado su inventario de bienes y derechos, tanto de los propios como de los bienes del Patrimonio del Estado adscritos a dicha entidad, que se revisará anualmente, con referencia al 31 de diciembre, y se someterá a la aprobación de la Presidencia de la Agencia Española de Protección de Datos. El inventario y sus modificaciones se remitirán anualmente al Ministerio de Hacienda en el primer mes de cada año natural.

5. Los bienes que el Estado adscriba a la Agencia quedarán afectados a su servicio y conservarán la calificación jurídica originaria, debiendo ser utilizados exclusivamente para los fines que determinaron la adscripción.

6. La persona titular de la Presidencia podrá acordar la innecesariedad para el servicio de los bienes muebles y, en su caso, la enajenación, cesión gratuita o destrucción del material no útil, así como cualesquiera otros de igual naturaleza, aplicando su producto a los fines propios de la Agencia.

Artículo 43. Contratación.

1. La actividad contractual de la Agencia Española de Protección de Datos queda sujeta a la Ley 9/2017, de 8 de noviembre, así como a su normativa de desarrollo.

2. A los citados efectos, aplicará el régimen previsto en las citadas normas para las Administraciones Públicas.

3. El órgano de contratación de la Agencia Española de Protección de Datos es la Presidencia, quien podrá delegar esta competencia salvo para contratos cuyo valor estimado fuera igual o superior a 120.000 euros.

4. La Agencia podrá acordar su adhesión a sistemas de contratación centralizada o la cofinanciación conjunta de contratos con el Ministerio de Hacienda cuando de ello resultase una mayor eficiencia en la asignación de recursos.

5. La Agencia recibirá las facturas electrónicas que emitan sus proveedores a través del punto general de entrada de facturas electrónicas correspondiente a la Administración General del Estado, en los términos previstos en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

Sección 2.^a Régimen presupuestario, de contabilidad y control económico-financiero

Artículo 44. Presupuestos.

1. La Agencia Española de Protección de Datos elaborará y aprobará anualmente su presupuesto, con la estructura que establezca el Ministerio de Hacienda y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El presupuesto de la Agencia tendrá carácter limitativo por su importe global y carácter estimativo para la distribución de los créditos por categorías económicas, con excepción de los correspondientes a gastos de personal que, en todo caso, tendrán carácter limitativo y vinculante por su cuantía total, y de los créditos que establezcan asignaciones identificando receptor o beneficiario, salvo las destinadas a atender transferencias corrientes o de capital al exterior, y las atenciones protocolarias y representativas, que tendrán carácter limitativo y vinculante, cualquiera que sea el nivel de la clasificación económica al que se establezcan.

3. La ejecución y modificación del presupuesto de la Agencia Española de Protección de Datos se regirán por las disposiciones de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que le sean de aplicación. La ejecución del presupuesto de la Agencia corresponde a su Presidencia.

4. El régimen de modificaciones de los créditos del presupuesto se ajustará a lo siguiente:

a) Las modificaciones del presupuesto de la Agencia serán autorizadas por la Presidencia de la Agencia Española de Protección de Datos cuando no incrementen la cuantía global del presupuesto, salvo que afecten a los créditos para gastos de personal, en cuyo caso la autorización será competencia del titular del Ministerio de Hacienda.

b) Corresponde igualmente a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen un incremento de hasta un tres por ciento de los créditos iniciales de su presupuesto total de gastos cuando sean consecuencia de necesidades surgidas durante el ejercicio, y siempre que no se incrementen los créditos para gastos de personal, en cuyo caso será competencia del titular del Ministerio de Hacienda.

c) Corresponde al titular del Ministerio de Hacienda autorizar las modificaciones presupuestarias que impliquen un incremento por encima del tres por ciento de los créditos iniciales del presupuesto de la Agencia y siempre que no excedan de un cinco por ciento.

d) Corresponde al Gobierno las modificaciones que impliquen un incremento por encima del cinco por ciento de los créditos iniciales del presupuesto de la Agencia.

e) Si la modificación afectase a aportaciones estatales recogidas en los Presupuestos Generales del Estado, la competencia para autorizar ambas modificaciones corresponderá a la autoridad que tuviera atribuida la modificación en el Presupuesto del Estado. Estas modificaciones no computarán a efectos de los porcentajes recogidos en las letras a) y b) anteriores.

5. La Agencia Española de Protección de Datos podrá disponer de cuentas bancarias de gestión para todo tipo de ingresos y pagos en el Banco de España y en la banca comercial.

6. La Agencia podrá adquirir compromisos de gasto que hayan de extenderse a ejercicios posteriores a aquel en que se autoricen, con los límites y previsiones que le sean establecidos por ley.

7. Se dará cuenta de las modificaciones adoptadas por la Presidencia, en función de las competencias atribuidas en el apartado 4, a la Dirección General de Presupuestos, del Ministerio de Hacienda, para su toma de razón.

Artículo 45. Contabilidad.

1. La Agencia deberá aplicar los principios contables públicos previstos en el artículo 122 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, así como el desarrollo de los principios y las normas establecidos en el Plan General de Contabilidad Pública, aprobado por Orden EHA/1037/2010, de 13 de abril, para lo cual contará con un sistema de información económico-financiero y presupuestario que tenga por objeto mostrar, a través de estados e informes, la imagen fiel del patrimonio, de la situación financiera, de los resultados y de la ejecución del presupuesto, que proporcione información de los costes sobre su actividad que sea suficiente para una correcta y eficiente adopción de decisiones.

2. La Intervención General de la Administración del Estado establecerá los requerimientos funcionales y, en su caso, los procedimientos informáticos que deberán observarse para cumplir lo dispuesto en el apartado anterior. En concreto, la Agencia aplicará, para la gestión contable, el sistema de información contable de la Administración General del Estado y sus organismos públicos, y suscribirá el correspondiente convenio con la Intervención General de la Administración del Estado para la utilización del sistema de apoyo a la gestión de las entidades públicas administrativas y del sistema de contabilidad analítica normalizada para organizaciones administrativas.

3. El ejercicio anual se computará por años naturales, comenzando el día 1 del mes de enero de cada año.

4. La Agencia contará con un sistema de contabilidad de gestión que permita efectuar el seguimiento del cumplimiento de los compromisos asumidos.

Artículo 46. Cuentas anuales.

1. La persona titular de la Presidencia formulará las cuentas anuales en un plazo de tres meses desde el cierre del ejercicio económico. Una vez auditadas por la Intervención General de la Administración del Estado, serán aprobadas dentro del primer semestre del año siguiente al que se refieran.

2. La Presidencia rendirá las cuentas anuales al Tribunal de Cuentas, por conducto de la Intervención General de la Administración del Estado, en el plazo de los siete meses siguientes a la terminación del ejercicio económico y una vez aprobadas.

Artículo 47. Control de la gestión económico-financiera.

1. El control externo de la gestión económico-financiera de la Agencia corresponderá al Tribunal de Cuentas, de acuerdo con su normativa específica.

2. El control interno de la gestión económico-financiera corresponderá a la Intervención General de la Administración del Estado, realizándose bajo las modalidades de control financiero permanente y de auditoría pública, en las condiciones y en los términos establecidos en la Ley 47/2003, de 26 de noviembre, a través de la Intervención Delegada en la Agencia.

CAPÍTULO V

Asesoramiento jurídico de la Agencia Española de Protección de Datos

Artículo 48. *Asistencia jurídica.*

La asistencia jurídica de la Agencia Española de Protección de Datos, consistente en el asesoramiento jurídico y en la representación y defensa en juicio, corresponde a la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, mediante la formalización del oportuno convenio en los términos previstos en la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica al Estado e Instituciones Públicas, y su normativa de desarrollo.

§ 2

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2018-16673

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus

órigenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también

riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones

tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la ley.*

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Artículo 3. *Datos de las personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. *Exactitud de los datos.*

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

- a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. *Deber de confidencialidad.*

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6. *Tratamiento basado en el consentimiento del afectado.*

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7. *Consentimiento de los menores de edad.*

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9. *Categorías especiales de datos.*

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. *Tratamiento de datos de naturaleza penal.*

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

Artículo 11. *Transparencia e información al afectado.*

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.
- c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

- a) Las categorías de datos objeto de tratamiento.
- b) Las fuentes de las que procedieran los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. *Disposiciones generales sobre ejercicio de los derechos.*

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. *Derecho de acceso.*

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales

que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. *Derecho de rectificación.*

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. *Derecho de supresión.*

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. *Derecho a la limitación del tratamiento.*

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. *Derecho de oposición.*

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20. *Sistemas de información crediticia.*

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. *Tratamientos relacionados con la realización de determinadas operaciones mercantiles.*

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. *Tratamientos con fines de videovigilancia.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. *Sistemas de exclusión publicitaria.*

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Artículo 24. *Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.*

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se registrarán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Artículo 25. *Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de

Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. *Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.*

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. *Tratamiento de datos relativos a infracciones y sanciones administrativas.*

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. *Obligaciones generales del responsable y encargado del tratamiento.*

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.*

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del

Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. *Encargado del tratamiento.*

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

- a) Los colegios profesionales y sus consejos generales.
- b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
- c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
- d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
- e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
- f) Los establecimientos financieros de crédito.
- g) Las entidades aseguradoras y reaseguradoras.
- h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
- i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.
- k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.
- l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.
Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.
- m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. *Cualificación del delegado de protección de datos.*

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. *Posición del delegado de protección de datos.*

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su

caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. *Códigos de conducta.*

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el

Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. *Acreditación de instituciones de certificación.*

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. *Régimen de las transferencias internacionales de datos.*

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. *Supuestos de adopción por la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. *Supuestos sometidos a autorización previa de las autoridades de protección de datos.*

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. *Supuestos sometidos a información previa a la autoridad de protección de datos competente.*

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. *Disposiciones generales.*

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. *Régimen económico presupuestario y de personal.*

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. *Funciones y potestades de la Agencia Española de Protección de Datos.*

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurren en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

- a) Incumplimiento grave de sus obligaciones,
- b) incapacidad sobrevenida para el ejercicio de su función,
- c) incompatibilidad, o
- d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. *Consejo Consultivo de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

- a) Un Diputado, propuesto por el Congreso de los Diputados.
- b) Un Senador, propuesto por el Senado.
- c) Un representante designado por el Consejo General del Poder Judicial.
- d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.
- e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
- f) Un experto propuesto por la Federación Española de Municipios y Provincias.
- g) Un experto propuesto por el Consejo de Consumidores y Usuarios.
- h) Dos expertos propuestos por las Organizaciones Empresariales.
- i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.
- j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
- k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.
- l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.
- m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.
- n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.
- ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. *Publicidad.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los

artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos sancionadores y a los procedimientos de apercibimiento, las que archiven las actuaciones previas de investigación, las dictadas respecto de las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Sección 2.^a Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 53 bis. *Actuaciones de investigación a través de sistemas digitales.*

Las actuaciones de investigación podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre la Agencia Española de Protección de Datos y el inspeccionado. Además, deben garantizar la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Agencia y requerirá la conformidad del inspeccionado en relación con su uso y con la fecha y hora de su desarrollo.

Artículo 54. *Planes de auditoría.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. *Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. *Acción exterior.*

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. *Autoridades autonómicas de protección de datos.*

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. *Cooperación institucional.*

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. *Tratamientos contrarios al Reglamento (UE) 2016/679.*

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de

Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.^a Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. *Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.*

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. *Intervención en caso de tratamientos transfronterizos.*

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. *Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.*

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. *Régimen jurídico.*

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo.

4. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Será en este caso de aplicación lo dispuesto en los apartados 1, 2 y 3 de este artículo.

5. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de

los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

6. El transcurso de los plazos de tramitación a los que se refiere el apartado anterior se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Artículo 65. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento, al organismo de supervisión establecido para la aplicación de los códigos de conducta o al organismo que asuma las funciones de resolución extrajudicial de conflictos a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

Si como consecuencia de dichas actuaciones de remisión, el responsable o encargado del tratamiento demuestra haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá inadmitir a trámite la reclamación.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos, sin perjuicio de la facultad de la Agencia de archivar posteriormente y de forma expresa la reclamación.

En el supuesto de que la Agencia Española de Protección de Datos actúe como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.4 de esta ley orgánica, el cómputo del plazo señalado en el párrafo anterior se iniciará una vez que se reciba en la Agencia toda la documentación necesaria para su tramitación.

Cuando los hechos de una reclamación relativa a la posible existencia en el ámbito competencial de la Agencia, guarden identidad sustancial con los que sean objeto de unas actuaciones previas de investigación o de un procedimiento sancionador ya iniciado, en la notificación de la decisión de admisión a trámite se podrá indicar el número de expediente

correspondiente a las actuaciones previas o al procedimiento correspondiente, así como de la dirección web en la que se publicará la resolución que ponga fin al mismo, a efectos de que el reclamante pueda conocer el curso y resultado de la investigación.

6. Tras la admisión a trámite, si el responsable o encargado del tratamiento demuestran haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá resolver el archivo de la reclamación, cuando en el caso concreto concurren circunstancias que aconsejen la adopción de otras soluciones más moderadas o alternativas a la acción correctiva, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos regulados en esta ley orgánica.

Artículo 66. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 64.4 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que impliquen un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 2.^a del capítulo I del título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa.

Artículo 68. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. *Medidas provisionales y de garantía de los derechos.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de

Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

- a) Los responsables de los tratamientos.
- b) Los encargados de los tratamientos.
- c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
- d) Las entidades de certificación.
- e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. *Infracciones.*

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. *Infracciones consideradas muy graves.*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

- a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
- b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
- c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.
- d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurren las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. *Infracciones consideradas graves.*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. Infracciones consideradas leves.

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificadas, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al

tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. *Interrupción de la prescripción de la infracción.*

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del acuerdo de inicio.

Artículo 76. *Sanciones y medidas correctivas.*

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
- f) La afectación a los derechos de los menores.
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.

4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.

Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

- a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
- b) Los órganos jurisdiccionales.
- c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
- d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
- e) Las autoridades administrativas independientes.
- f) El Banco de España.
- g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
- h) Las fundaciones del sector público.
- i) Las Universidades Públicas.
- j) Los consorcios.
- k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Artículo 78. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

- a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.
- b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.
- c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. *Los derechos en la Era digital.*

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet.*

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.
2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.
3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.
4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.
5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.
6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital.*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia

así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet.*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. *Protección de datos y transparencia y acceso a la información pública.*

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. *Cómputo de plazos.*

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. *Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.*

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

- a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;
- b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o
- c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. *Incorporación de deudas a sistemas de información crediticia.*

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. *Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.*

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. *Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.*

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. *Privacidad en las comunicaciones electrónicas.*

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. *Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.*

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Disposición adicional decimosexta. *Prácticas agresivas en materia de protección de datos.*

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. *Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

- a) La Ley 14/1986, de 25 de abril, General de Sanidad.
- b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.
- c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.
- g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.
- h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.
- i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.
- j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

- a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. *Criterios de seguridad.*

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. *Derechos de los menores ante Internet.*

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. *Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.*

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. *Educación digital.*

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. *Acceso a los archivos públicos y eclesiásticos.*

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición adicional vigésima tercera. *Modelos de presentación de reclamaciones.*

La Agencia Española de Protección de Datos podrá establecer modelos de presentación de reclamaciones ante la misma en todos los ámbitos en los que ésta tenga competencia, que serán de uso obligatorio para los interesados independientemente de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas.

Los modelos serán publicados en el "Boletín Oficial del Estado" y en la Sede Electrónica de la Agencia Española de Protección de Datos y serán de obligado cumplimiento al mes de su publicación en el "Boletín Oficial del Estado".»

Disposición transitoria primera. *Estatuto de la Agencia Española de Protección de Datos.*

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. *Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. *Tratamientos sometidos a la Directiva (UE) 2016/680.*

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. [Ref. BOE-A-2021-8806](#)

Disposición transitoria quinta. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. *Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.*

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concorra alguna de las circunstancias siguientes:

- a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.
- b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. *Derogación normativa.*

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. *Naturaleza de la presente ley.*

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

- El Título IV,
- el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,
- el Título VIII,
- el Título IX,
- los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,
- las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,
- las disposiciones transitorias,
- y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. *Título competencial.*

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.^a de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.^a y 18.^a de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.^a de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.^a de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.^a de la Constitución.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.*

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

«3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

«Artículo cincuenta y ocho bis. *Utilización de medios tecnológicos y datos personales en las actividades electorales.*

1. (Anulado)

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Disposición final cuarta. *Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. [...]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[...]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.*

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal

podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«**Artículo 15 bis.** *Intervención en procesos de defensa de la competencia y de protección de datos.*

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

§ 2 Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«**Artículo 16.** [...]»

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. *Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.*

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. Registro de actividades de tratamiento.

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevaran la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

«Artículo 28. [...]

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. *Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.*

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

«**Artículo 20 bis.** *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. *Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.*

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

«j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. *Desarrollo normativo.*

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. *Entrada en vigor.*

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 3

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales

Jefatura del Estado
«BOE» núm. 126, de 27 de mayo de 2021
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2021-8806

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica:

PREÁMBULO

I

La Unión Europea es un espacio en el que los estándares y las garantías de protección de los derechos de las personas físicas a la protección de los datos personales se encuentran en la vanguardia internacional y constituyen un referente mundial. El rápido desarrollo tecnológico, especialmente de Internet, así como la creciente globalización de la economía mundial y europea han hecho imprescindible abordar la reforma del marco jurídico de la protección de datos, al objeto de consolidar e incluso mejorar este elevado nivel de protección a través de la creación de un marco legislativo nuevo, adaptado a la realidad cambiante, al tiempo que sólido, coherente e integral. En definitiva, un entorno normativo para un mundo globalizado y digital.

En este sentido, la Comunicación de la Comisión Europea «Un enfoque global de la protección de los datos personales en la Unión Europea», de 4 de noviembre de 2010, precedida de un intenso periodo de consultas durante más de dos años con los Estados miembros, el público en general, así como con los distintos sectores afectados, sentó las bases de lo que sería esta nueva perspectiva normativa.

El marco normativo resultante consta, principalmente, de dos instrumentos: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), que sustituye a una norma vigente

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

desde hacía más de veinte años, y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

En nuestro ordenamiento jurídico, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptó el Reglamento General de Protección de Datos, en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

II

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, objeto de transposición por esta Ley Orgánica, deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que había sido superada por varias razones.

En primer lugar, se trataba de una norma previa al Tratado de Lisboa que requería de su oportuna adaptación a los nuevos Tratados, en particular, al artículo 16 del Tratado de Funcionamiento de la Unión Europea, que exige que el Consejo y el Parlamento Europeo, a través del procedimiento legislativo ordinario, regulen la protección de los datos personales.

En segundo término, la decisión marco se aprobó conforme a la estructura de pilares de la Unión Europea, previa al Tratado de Lisboa, por lo que contaba con un ámbito de aplicación limitado exclusivamente al tratamiento de datos personales de carácter transfronterizo entre los Estados miembros, sin alcanzar, por tanto, a los tratamientos de carácter estrictamente nacional.

Asimismo, otorgaba una amplísima capacidad de maniobra a los Estados miembros, sin asegurar un nivel mínimo de armonización deseable en determinados ámbitos, como el reconocimiento en todos los Estados del derecho de acceso de los interesados a sus propios datos, el principio del tratamiento de los datos para fines determinados o las condiciones para las transferencias internacionales.

En definitiva, la fragmentación y complejidad de la regulación en este campo perjudicaba la necesaria confianza entre los actores de la cooperación policial y judicial penal en Europa, quienes mostraban recelos a compartir información, entre otros motivos, por la ausencia de una mínima armonización en cuanto a la protección de los datos de carácter personal; unos datos que resultan esenciales en el terreno de la cooperación operativa.

III

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, subsana estas deficiencias, ampliando su ámbito de aplicación al tratamiento nacional de los datos personales en el espacio de la cooperación policial y judicial penal. Toda vez que cubre otras carencias de la normativa europea anterior, dado que incluye la regulación de los datos genéticos –que reclamaba el Tribunal Europeo de Derechos Humanos–, así como la distinción entre los datos personales según su grado de exactitud y fiabilidad, o la diferenciación entre distintas categorías de interesados.

Resulta pertinente poner de relieve que la citada directiva que transpone esta Ley Orgánica se aprobó como respuesta a las crecientes amenazas para la seguridad en el contexto nacional e internacional, que tienen, en numerosos casos, un componente transfronterizo. Por esta razón, la cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los países implicados se convierten en un objetivo ineludible. En efecto, los atentados terroristas de Nueva York en 2001 supusieron un punto de inflexión en la necesidad de reforzar la cooperación judicial y policial en la lucha contra el terrorismo, como volvería a ponerse de manifiesto con ocasión de los atentados de Bruselas y Niza en 2016.

La cooperación encaminada a compartir a tiempo la información operativa precisa se erige en un requisito de eficacia en la prevención y lucha contra este tipo de amenazas. Todo

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

ello, teniendo en cuenta el estado de la técnica, que permite, en la actualidad, tratamientos de datos a gran escala en el ámbito de la seguridad.

Este intercambio de información debe realizarse, en todo caso, de manera que se garanticen los principios democráticos y la seguridad de las personas a lo largo de las fases del tratamiento.

En consecuencia, esta Ley Orgánica asume la finalidad de lograr un elevado nivel de protección de los derechos de la ciudadanía, en general, y de sus datos personales, en particular, que resulte homologable al del resto de los Estados miembros de la Unión Europea, incorporando y concretando las reglas que establece la directiva.

En este sentido, la Constitución española fue precursora del reconocimiento y la defensa del derecho fundamental a la protección de datos personales. Así, el artículo 18.4 de nuestra norma fundamental dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos. El Tribunal Constitucional, en reiterada jurisprudencia, entiende la protección de datos como un derecho fundamental que garantiza a toda persona la capacidad de controlar el uso y destino de sus datos, con el propósito de evitar el tráfico ilícito o lesivo de los mismos o una utilización para fines distintos de los que justificaron su obtención.

Por todo ello, la transposición de esta directiva por los Estados miembros supone el establecimiento de un marco jurídico consistente, que proporciona la seguridad jurídica necesaria para facilitar la cooperación policial y judicial penal y, por tanto, una mayor eficacia en el desempeño de sus funciones por las Fuerzas y Cuerpos de Seguridad y de nuestro sistema judicial penal en su conjunto, incluido el penitenciario.

IV

Esta Ley Orgánica consta de sesenta y cinco artículos estructurados en ocho capítulos, cinco disposiciones adicionales, una disposición transitoria, una disposición derogatoria y doce disposiciones finales.

El capítulo I, relativo a las disposiciones generales, define el objeto de la Ley Orgánica, entendiéndose como la regulación del tratamiento de los datos personales para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluida la protección y de prevención frente a las amenazas contra la seguridad pública, cuando dicho tratamiento se lleve a cabo por los órganos que, a efectos de esta Ley Orgánica, tengan la consideración de autoridades competentes.

La finalidad principal es que los datos sean tratados por estas autoridades competentes de manera que se cumplan los fines prevenidos a la par que establecer los mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos, de forma que se cumpla lo dispuesto en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea y el artículo 18.4 de la Constitución.

Asimismo, en correspondencia con lo que dispone el artículo 22.6 de la Ley Orgánica 3/2018, de 5 de diciembre, cuando el tratamiento de los datos personales se realice para alguno de los fines establecidos en esta Ley Orgánica y proceda de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, o bien se lleve a cabo por los órganos competentes para la vigilancia y control en los centros penitenciarios o para el control, regulación, vigilancia y disciplina del tráfico, dichos tratamientos se regularán por las disposiciones de esta Ley Orgánica complementándose, en lo que no resulte contrario a su contenido, con la normativa vigente que regula estos ámbitos. De este modo, se establece un nuevo sistema que gira en torno a las obligaciones de los responsables del tratamiento y a las distintas misiones que se les asignan.

Aunque se deben excluir con carácter general, se incluyen igualmente algunas previsiones específicas para el tratamiento de los datos de personas fallecidas a similitud de lo que se dispone en la precitada Ley Orgánica 3/2018, de 5 de diciembre.

Las autoridades competentes, a efectos de esta Ley Orgánica, se definen como autoridades públicas con competencias legalmente encomendadas para la consecución de los fines específicos incluidos en el ámbito de aplicación. En concreto, se determina que serán autoridades competentes: las Fuerzas y Cuerpos de Seguridad; las autoridades

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

judiciales del orden jurisdiccional penal y el Ministerio Fiscal; las Administraciones Penitenciarias; la Dirección Adjunta de Vigilancia Aduanera; el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias; y la Comisión de Vigilancia de Actividades de Financiación del Terrorismo. Todo ello, sin perjuicio de que los tratamientos que se lleven a cabo por los órganos jurisdiccionales se rijan por lo dispuesto en esta Ley Orgánica, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales penales.

Se excluyen expresamente del ámbito de aplicación ciertos tratamientos, como los realizados por las autoridades competentes para fines distintos de los cubiertos por la Ley Orgánica; los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito del capítulo II del título V del Tratado de la Unión Europea, en relación a la Política Exterior y de Seguridad Común; los derivados de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión Europea; y los sometidos a la normativa sobre materias clasificadas. Entre estos últimos se mencionan expresamente como incluidos los tratamientos relativos a la Defensa Nacional.

El capítulo II se refiere a los principios de protección de datos cuya garantía corresponde al responsable del tratamiento. Estos principios se regulan en términos similares a lo establecido en el Reglamento General de Protección de Datos, con algunas especialidades propias del ámbito de esta Ley Orgánica.

Se incluye un deber de colaboración con las autoridades competentes, según el cual, salvo que legalmente sea exigible una autorización judicial, las Administraciones Públicas o cualquier persona física o jurídica deberá proporcionar a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial la información necesaria para la investigación o enjuiciamiento de infracciones penales o la ejecución de las penas y la información necesaria para la protección y prevención frente a un peligro real y grave para la seguridad pública. Todo ello, con la obligación de no informar al interesado de dichos tratamientos ulteriores. Esta última precisión resulta fundamental para evitar que la puesta de la información a disposición del interesado pueda poner en peligro los fines que, de acuerdo con la directiva y esta Ley Orgánica, justifican el tratamiento de los datos.

Se regulan, también, los plazos de conservación y de revisión de los datos de carácter personal tratados, siendo relevante el establecimiento de un plazo máximo de conservación de los datos con carácter general y la implantación de un sistema que permite al responsable revisar, en el plazo que el mismo establezca dentro del margen legal, la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de sus actividades de tratamiento. El responsable deberá, en sus tratamientos, distinguir los datos que correspondan a las diversas categorías de interesados, tales como los sospechosos, los condenados o los sancionados, las víctimas o los terceros involucrados, así como diferenciar, en la medida de lo posible, si los datos que trata son datos basados en hechos o en apreciaciones.

Se exigen igualmente ciertas condiciones que determinan la licitud de todo tratamiento de datos de carácter personal, esto es, que sean tratados por las autoridades competentes; que resulten necesarios para los fines de esta Ley Orgánica y que, en caso necesario y en cada ámbito particular, se especifiquen las especialidades por una norma con rango de ley que incluya unos contenidos mínimos.

En el supuesto de transmisión de datos sujetos a condiciones específicas de tratamiento, dichas condiciones deberán ser respetadas por el destinatario de los mismos, en especial, la prohibición de transmitirlos o de utilizarlos para fines distintos para los que fueron transmitidos.

De igual modo, se exige que el tratamiento de categorías especiales de datos, como son los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical o los genéticos o biométricos, sólo pueda tener lugar cuando sea estrictamente necesario y se cumplan ciertas condiciones.

Los datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidos en esta categoría especial cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Esta necesidad de identificación en las actuaciones amparadas legalmente se lleva a cabo, con frecuencia, por las distintas autoridades competentes. El propósito es singularizar los autores o partícipes de infracciones penales,

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

así como poder reconocer si son las personas que se supone o se busca, y de esta forma, atribuir o exonerar, sin género de dudas, la participación en determinados hechos, gracias a posibles indicios o vestigios biométricos.

Habida cuenta de la vertiginosa evolución tecnológica y los medios electrónicos de los que se dispone, se incluye la habilitación legal que facilite una respuesta rápida y adecuada en el uso de estos datos, con el objetivo final de garantizar y proteger los derechos de los interesados y de la ciudadanía en general.

Se prohíbe, igualmente, la adopción de decisiones individuales automatizadas, incluida la elaboración de perfiles en este ámbito, salvo que esté autorizado por una norma con rango de ley del ordenamiento jurídico español o europeo.

El capítulo III, se divide en dos secciones y aborda los derechos de las personas. Regula una serie de condiciones generales del ejercicio de los derechos, tales como la obligación exigible al responsable de facilitar la información correspondiente a los derechos del interesado de forma concisa, con un lenguaje claro y sencillo y de manera gratuita. Se establece la información que debe ponerse a disposición del interesado, siendo algunos datos obligatorios, en todo caso, y otros en casos concretos.

Se reconocen los derechos de acceso, rectificación, supresión y limitación del tratamiento. En virtud de tales derechos se faculta al interesado a conocer si se están tratando o no sus datos y, en caso afirmativo, acceder a cierta información sobre el tratamiento; a obtener la rectificación de sus datos si estos resultaran inexactos; a suprimirlos cuando fueran contrarios a lo dispuesto en los artículos 6, 11 o 13, o cuando así lo requiera una obligación legal exigible al responsable; y a limitar el tratamiento, cuando el interesado ponga en duda la exactitud de los datos o estos datos deban conservarse únicamente a efectos probatorios.

Estos derechos podrán ser ejercidos por el interesado directamente o, en determinados casos, a través de la autoridad de protección de datos.

Dispone esta Ley Orgánica que estos derechos pueden ser restringidos por ciertas causas tasadas, como cuando sea necesario para evitar que se obstaculice una investigación o se ponga en peligro la seguridad pública o la seguridad nacional.

Se establece, en su sección segunda, un régimen especial de derechos de los interesados en el marco de investigaciones y procesos penales.

El capítulo IV recoge las obligaciones y responsabilidades de los responsables y encargados de protección de datos, las medidas de seguridad y la figura del delegado de protección de datos, a lo largo de tres secciones. El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas.

El encargado del tratamiento llevará a cabo sus funciones por cuenta del responsable, debiendo ofrecer garantías para aplicar medidas técnicas y organizativas apropiadas.

Todo responsable y encargado del tratamiento deberá conservar un registro de actividades de tratamiento, con datos identificativos, tales como los datos de contacto del responsable, los fines o las categorías de interesados, y un registro de operaciones, pieza angular de este sistema e instrumento básico para acreditar el cumplimiento de varios de los principios de tratamiento, que comprenderá la recogida, la alteración, las consultas y las transferencias de los datos personales entre otras operaciones. Asimismo, están obligados a cooperar con la autoridad de protección de datos, en el marco de la legislación vigente.

Se establecen ciertas obligaciones que responden a un nuevo modelo de responsabilidad activa que exige una valoración previa del riesgo que pudiera generar el tratamiento de los datos de carácter personal para los interesados, para, a partir de dicha valoración, adoptar las medidas que procedan.

Se presta una atención detallada a la seguridad del tratamiento, regulándose alguna de las medidas de seguridad que se aplicarán, si bien solo se dispone como obligatoria la puesta en marcha del citado registro de operaciones como medida técnica y organizativa, siendo las demás las que el responsable determine como las más adecuadas para lograr el control que se le solicita en virtud del tipo de tratamiento que se esté llevando a cabo y del nivel de riesgo que se estime, tras el correspondiente análisis. Se impone, asimismo, el deber de notificación a la autoridad de protección de datos de cualquier violación de la

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

seguridad que, con carácter general, deberá ser notificada al interesado, salvo en supuestos expresamente previstos en la ley.

El delegado de protección de datos se configura como el órgano o figura de asesoramiento y supervisión de los responsables de protección de datos, que podrá ser único para varias autoridades competentes y cuya designación será obligatoria salvo en relación con los tratamientos de datos con fines jurisdiccionales. En el caso de que se dispongan tratamientos que queden bajo distintos ámbitos de aplicación, con el fin de evitar disfunciones en las organizaciones de las autoridades competentes, se establece que la figura del delegado de protección de datos será única para todos ellos.

El capítulo V regula las transferencias de datos personales realizadas por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea u otra organización internacional y se establecen las condiciones que deberán cumplirse para que estas sean lícitas.

Así, con el fin de garantizar que no se menoscabe el nivel de protección de las personas físicas previsto en esta Ley Orgánica, la transferencia respetará ciertas condiciones previstas en la misma. De este modo, sólo deben realizarse cuando sean necesarias para los fines de esta Ley Orgánica y cuando el responsable del tratamiento en el tercer país u organización internacional sea autoridad competente en relación a dichos fines.

Asimismo, cuando el dato se transfiere a un tercer país o a una organización internacional, la autoridad competente del Estado miembro en el que se obtuvo el dato, debe autorizar previamente esta transferencia y las ulteriores que puedan tener lugar a otro tercer país o a una organización internacional. En cuanto al tercer país u organización internacional destinatario de la transferencia, deberá ser objeto de evaluación por la Comisión Europea a la vista de su nivel de protección de datos o, en caso de ausencia de decisión, debe entenderse por el responsable del tratamiento que ofrece garantías adecuadas. Sólo por las causas excepcionales previstas en esta Ley Orgánica se podrán autorizar transferencias fuera de estos supuestos. Este capítulo finaliza con la regulación de la transferencia internacional de datos personales a destinatarios que, no siendo autoridades competentes, están establecidos en terceros países.

El capítulo VI, relativo a las autoridades de protección de datos, dispone que dichas autoridades sean la Agencia Española de Protección de Datos y las Agencias Autonómicas de Protección de Datos, en sus respectivos ámbitos competenciales. Asimismo, la Ley Orgánica recoge sus potestades, funciones y la asistencia entre autoridades de protección de datos de los Estados miembros. Se remite en lo restante a la normativa que les resulte de aplicación.

El capítulo VII prevé que los procedimientos de reclamación que se planteen ante las autoridades de protección de datos se rijan por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, o, en su caso, por la normativa reguladora de la autoridad de protección de datos correspondiente. Se refiere a aquellos supuestos en que los responsables o encargados del tratamiento, o de la autoridad de protección de datos, en su caso, incumplan esta Ley Orgánica y generen un daño o lesión en los bienes o derechos del interesado.

Este capítulo, además, aborda la responsabilidad de los responsables o encargados del tratamiento o de la autoridad de protección de datos, en su caso, cuando incumplan esta Ley Orgánica y se genere un daño o lesión en los bienes o derechos de un interesado. De igual modo, se detalla la forma de ejercer el derecho a la tutela judicial efectiva ante la jurisdicción contencioso-administrativa contra las decisiones de una autoridad de protección de datos que puedan entenderse que conciernen a los interesados.

Finalmente, el capítulo VIII regula el régimen sancionador específico aplicable ante incumplimientos de las obligaciones previstas en esta Ley Orgánica. Se definen los sujetos sobre los que recaerá la responsabilidad por las infracciones cometidas. Se determinan las reglas del concurso de normas para resolver los casos en los que un hecho pueda ser calificado con arreglo a dos o más de ellas, al tiempo que se tipifican las infracciones, que, en función de su gravedad, podrán ser leves, graves o muy graves. Por último, se establecen las sanciones que se pueden imponer, y se fijan los plazos de prescripción tanto de las infracciones como de las sanciones y de caducidad.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

Las disposiciones adicionales se refieren a regímenes específicos, al intercambio de datos dentro de la Unión Europea, a los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial, y a los tratamientos que se efectúen en relación con los ficheros y al Registro de Población de las Administraciones Públicas.

Las disposiciones finales introducen las modificaciones necesarias en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, para adecuarla a las previsiones de esta Ley Orgánica en relación con los tratamientos para ejecución de la pena; en la Ley 50/1981, de 30 de diciembre; en la Ley Orgánica 6/1985, de 1 de julio; en la Ley Orgánica 3/2018, de 5 de diciembre; en la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves en correspondencia con determinadas obligaciones de los operadores; en la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte; en la Ley 5/2014, de 4 de abril, de Seguridad Privada para adecuar, en ambos casos, los plazos de caducidad de los expedientes sancionadores; y en el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre, para dar soporte legal específico a las matriculaciones por razones de Seguridad Nacional.

En la elaboración de esta Ley Orgánica se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, exigidos por el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, se trata de una norma necesaria, dado que la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, exige una ley de carácter orgánico, al afectar la norma comunitaria a un derecho fundamental reconocido en el artículo 18 de la Constitución y por imperativo del artículo 81 de la misma. En este sentido, el artículo 18.4 de la Constitución dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de la ciudadanía y el pleno ejercicio de sus derechos.

Esta Ley Orgánica, además, incorpora a nuestro ordenamiento interno los instrumentos que permitirán una eficaz protección de los datos de las personas físicas frente a su tratamiento por parte de las autoridades competentes con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

Por lo que respecta al principio de seguridad jurídica, en razón de la materia objeto de regulación, la transposición de la directiva se realiza mediante una Ley Orgánica, cuya tramitación e integración en el ordenamiento jurídico goza de las garantías que amparan las normas de esta naturaleza.

En cuanto al principio de proporcionalidad, esta Ley Orgánica contempla un importante número de garantías orientadas a que el tratamiento de datos personales sea proporcional, oportuno, mínimo y suficiente para el cumplimiento de los fines que se persiguen. En particular, su tratamiento se sujeta a los principios que rigen el tratamiento de datos personales, por lo que se exige que no sean tratados para otros fines distintos de los establecidos en la norma, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por nuestro Derecho interno. Cuando los datos personales sean tratados para otros fines que no sean los de la prevención, detección, investigación o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, se aplicará el Reglamento General de Protección de Datos, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

Se cumple, también, el principio de transparencia, puesto que esta norma ha sido sometida a los correspondientes trámites de participación pública, esto es, el de consulta pública previa y el de audiencia e información pública.

En la tramitación de esta Ley Orgánica, además de los diversos Ministerios concernidos por razón de la materia, han emitido informe la Agencia Española de Protección de Datos; la Agencia Vasca de Protección de Datos; la Autoridad Catalana de Protección de Datos; el

Consejo Fiscal; el Consejo General del Poder Judicial; los Departamentos de Seguridad Pública del Gobierno Vasco y de Interior de la Generalidad de Cataluña; y finalmente el Consejo de Estado. Se trata, por tanto, de un texto en el cual se han incorporado las consideraciones de órganos tan relevantes como los expuestos.

Por último, esta Ley Orgánica se dicta al amparo de las reglas 1.^a, 6.^a, 18.^a y 29.^a del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; sobre legislación penal, penitenciaria y procesal; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; y en materia de seguridad pública.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Esta Ley Orgánica tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 2. *Ámbito de aplicación.*

1. Será de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública.

2. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de las actuaciones o procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, en el ámbito del artículo 1, se regirá por lo dispuesto en la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las leyes procesales que le sean aplicables y, en su caso, por la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal. Las autoridades de protección de datos a las que se refiere el capítulo VI no serán competentes para controlar estas operaciones de tratamiento.

3. Quedan fuera del ámbito de aplicación de esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los realizados por las autoridades competentes para fines distintos de los previstos en el artículo 1, incluidos los fines de archivo por razones de interés público, investigación científica e histórica o estadísticos. Estos tratamientos se someterán plenamente a lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

b) Los llevados a cabo por los órganos de la Administración General del Estado en el marco de las actividades comprendidas en el ámbito de aplicación del capítulo II del título V del Tratado de la Unión Europea.

c) Los tratamientos que afecten a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

d) Los sometidos a la normativa sobre materias clasificadas, entre los que se encuentran los tratamientos relativos a la Defensa Nacional.

e) Los tratamientos realizados en las acciones civiles y procedimientos administrativos o de cualquier índole vinculados con los procesos penales que no tengan como objetivo directo ninguno de los fines del artículo 1.

4. Esta Ley Orgánica no se aplicará a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo siguiente.

Artículo 3. *Datos de personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso, rectificación o supresión de los datos de aquel. Estos derechos se regularán de acuerdo con lo dispuesto en esta Ley Orgánica.

2. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona interesada.

3. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el apartado anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Artículo 4. *Autoridades competentes.*

1. Será autoridad competente, a los efectos de esta Ley Orgánica, toda autoridad pública que tenga competencias encomendadas legalmente para el tratamiento de datos personales con alguno de los fines previstos en el artículo 1.

En particular, tendrán esa consideración, en el ámbito de sus respectivas competencias, las siguientes autoridades:

- a) Las Fuerzas y Cuerpos de Seguridad.
- b) Las Administraciones Penitenciarias.
- c) La Dirección Adjunta de Vigilancia Aduanera de la Agencia Estatal de Administración Tributaria.
- d) El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias.
- e) La Comisión de Vigilancia de Actividades de Financiación del Terrorismo.

2. También tendrán consideración de autoridades competentes las Autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Artículo 5. *Definiciones.*

A efectos de esta Ley Orgánica se entenderá por:

a) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

b) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

c) «limitación del tratamiento»: el marcado de los datos personales conservados con el fin de limitar su tratamiento en el futuro;

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

d) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

e) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

f) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o dispersado de forma funcional o geográfica;

g) «responsable del tratamiento» o «responsable»: la autoridad competente que sola o conjuntamente con otras, determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión Europea o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento.

h) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

i) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerará destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con la legislación española o de la Unión Europea; el tratamiento de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

j) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma;

k) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de la persona física de que se trate;

l) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o de conducta de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

m) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

n) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

CAPÍTULO II

Principios, licitud del tratamiento y videovigilancia

Sección 1.ª Principios y licitud del tratamiento

Artículo 6. *Principios relativos al tratamiento de datos personales.*

1. Los datos personales serán:

a) Tratados de manera lícita y leal.

b) Recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

c) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.

d) Exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que son tratados.

e) Conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados.

f) Tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas.

2. Los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión Europea o por la legislación española. Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión Europea.

3. Los datos personales podrán ser tratados por el mismo responsable o por otro, para fines establecidos en el artículo 1 distintos de aquel para el que hayan sido recogidos, en la medida en que concurran cumulativamente las dos circunstancias siguientes:

a) Que el responsable del tratamiento sea competente para tratar los datos para ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

b) Que el tratamiento sea necesario y proporcionado para la consecución de ese otro fin, de acuerdo con el Derecho de la Unión Europea o la legislación española.

4. El tratamiento por el mismo responsable o por otro podrá incluir el archivo por razones de interés público, y el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, con sujeción a las garantías adecuadas para los derechos y libertades de los interesados.

5. El responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo.

Artículo 7. Deber de colaboración.

1. Las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes, antecedentes y justificantes que les soliciten y que sean necesarios para la investigación y enjuiciamiento de infracciones penales o para la ejecución de las penas. La petición de la Policía Judicial se deberá ajustar exclusivamente al ejercicio de las funciones que le encomienda el artículo 549.1 de la Ley Orgánica 6/1985, de 1 de julio y deberá efectuarse siempre de forma motivada, concreta y específica, dando cuenta en todo caso a la autoridad judicial y fiscal.

La comunicación de datos, informes, antecedentes y justificantes por la Administración Tributaria, la Administración de la Seguridad Social y la Inspección de Trabajo y Seguridad Social, se efectuará de acuerdo con su legislación respectiva.

2. En los restantes casos, las Administraciones públicas, así como cualquier persona física o jurídica, proporcionarán los datos, informes, antecedentes y justificantes a las autoridades competentes que los soliciten, siempre que estos sean necesarios para el desarrollo específico de sus misiones para la prevención, detección e investigación de infracciones penales y para la prevención y protección frente a un peligro real y grave para la seguridad pública. La petición de la autoridad competente deberá ser concreta y específica y contener la motivación que acredite su relación con los indicados supuestos.

3. No será de aplicación lo dispuesto en los apartados anteriores cuando legalmente sea exigible la autorización judicial para recabar los datos necesarios para el cumplimiento de los fines del artículo 1.

4. En los supuestos contemplados en los apartados anteriores, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, a fin de garantizar la actividad investigadora.

Con el mismo propósito, los sujetos a los que el ordenamiento jurídico imponga un deber específico de colaboración con las autoridades competentes para el cumplimiento de los fines establecidos en el artículo 1, no informarán al interesado de la transmisión de sus datos a dichas autoridades, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma, en cumplimiento de sus obligaciones específicas.

Artículo 8. *Plazos de conservación y revisión.*

1. El responsable del tratamiento determinará que la conservación de los datos personales tenga lugar sólo durante el tiempo necesario para cumplir con los fines previstos en el artículo 1.

2. El responsable del tratamiento deberá revisar la necesidad de conservar, limitar o suprimir el conjunto de los datos personales contenidos en cada una de las actividades de tratamiento bajo su responsabilidad, como máximo cada tres años, atendiendo especialmente en cada revisión a la edad del afectado, el carácter de los datos y a la conclusión de una investigación o procedimiento penal. Si es posible, se hará mediante el tratamiento automatizado apropiado.

3. Con carácter general, el plazo máximo para la supresión de los datos será de veinte años, salvo que concurran factores como la existencia de investigaciones abiertas o delitos que no hayan prescrito, la no conclusión de la ejecución de la pena, reincidencia, necesidad de protección de las víctimas u otras circunstancias motivadas que hagan necesario el tratamiento de los datos para el cumplimiento de los fines del artículo 1.

Artículo 9. *Distinción entre categorías de interesados.*

El responsable del tratamiento, en la medida de lo posible, establecerá entre los datos personales de las distintas categorías de interesados, distinciones tales como:

- a) Personas respecto de las cuales existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en la comisión de una infracción penal.
- b) Personas condenadas o sancionadas por una infracción penal.
- c) Víctimas o afectados por una infracción penal o que puedan serlo.
- d) Terceros involucrados en una infracción penal como son: personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones o procesos penales ulteriores, personas que puedan facilitar información sobre dichas infracciones, o personas de contacto o asociados de una de las personas mencionadas en las letras a) y b).

Lo anterior no debe impedir la aplicación del derecho a la presunción de inocencia tal como lo garantiza el artículo 24 de la Constitución.

Artículo 10. *Verificación de la calidad de los datos personales.*

1. El responsable del tratamiento, en la medida de lo posible, establecerá una distinción entre los datos personales basados en hechos y los basados en apreciaciones personales.

2. Las autoridades competentes adoptarán todas las medidas razonables para garantizar que los datos personales que sean inexactos, incompletos o no estén actualizados, no se transmitan ni se pongan a disposición de terceros. En toda transmisión de datos se trasladará al mismo tiempo la valoración de su calidad, exactitud y actualización.

En la medida de lo posible, en todas las transmisiones de datos personales se añadirá la información necesaria para que la autoridad competente receptora pueda valorar hasta qué punto son exactos, completos y fiables, y en qué medida están actualizados. Igualmente, la autoridad competente transmisora, en la medida en que sea factible, controlará la calidad de los datos personales antes de transmitirlos o ponerlos a disposición de terceros.

3. Si se observara que los datos personales transmitidos son incorrectos o que se han transmitido ilegalmente, estas circunstancias se pondrán en conocimiento del destinatario sin dilación indebida. En tal caso, los datos deberán rectificarse o suprimirse, o el tratamiento deberá limitarse de conformidad con lo previsto en el artículo 23.

Artículo 11. *Licitud del tratamiento.*

1. El tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de sus funciones.

2. Cualquier ley que regule tratamientos de datos personales para los fines incluidos dentro del ámbito de aplicación de esta Ley Orgánica deberá indicar, al menos, los objetivos del tratamiento, los datos personales que vayan a ser objeto del mismo y las finalidades del tratamiento.

Artículo 12. *Condiciones específicas de tratamiento.*

1. Cuando el Derecho de la Unión Europea o la legislación española prevea condiciones específicas aplicables al tratamiento, la autoridad competente transmitente deberá informar al destinatario al que se transmitan los datos, de dichas condiciones y de la obligación de respetarlas.

2. Las condiciones específicas de tratamiento podrán ser, entre otras, la prohibición de transmisión de datos o de su utilización para fines distintos para los que fueron transmitidos o, en caso de limitación del derecho a la información, la prohibición de dar información al interesado sin la autorización previa de la autoridad transmisora.

3. La autoridad competente transmitente no aplicará a los destinatarios de otros Estados miembros de la Unión Europea o de organismos, agencias y órganos establecidos en virtud de los capítulos 4 y 5 del título V de la tercera parte del Tratado de Funcionamiento de la Unión Europea, condiciones distintas de las aplicables a las transmisiones de datos similares dentro de España.

Artículo 13. *Tratamiento de categorías especiales de datos personales.*

1. El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:

- a) Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.
- b) Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.
- c) Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

2. Las autoridades competentes, en el marco de sus respectivas funciones y competencias, podrán tratar datos biométricos dirigidos a identificar de manera unívoca a una persona física con los fines de prevención, investigación, detección de infracciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

3. Los datos de los menores de edad y de las personas con capacidad modificada judicialmente o que estén incurso en procesos de dicha naturaleza, se tratarán garantizando el interés superior de los mismos y con el nivel de seguridad adecuado.

Artículo 14. *Mecanismo de decisión individual automatizado.*

1. Están prohibidas las decisiones basadas únicamente en un tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos negativos para el interesado o que le afecten significativamente, salvo que se autorice expresamente por una norma con rango de ley o por el Derecho de la Unión Europea. La norma habilitante del tratamiento deberá establecer las medidas adecuadas para salvaguardar los derechos y libertades del interesado, incluyendo el derecho a obtener la intervención humana en el proceso de revisión de la decisión adoptada.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

2. Las decisiones a las que se refiere el apartado anterior no se basarán en las categorías especiales de datos personales contempladas en el artículo 13, salvo que se hayan tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

3. Queda prohibida la elaboración de perfiles que dé lugar a una discriminación de las personas físicas sobre la base de categorías especiales de datos personales establecidas en el artículo 13.

Sección 2.ª Tratamiento de datos personales en el ámbito de la videovigilancia por Fuerzas y Cuerpos de Seguridad

Artículo 15. *Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad.*

1. La captación, reproducción y tratamiento de datos personales por las Fuerzas y Cuerpos de Seguridad en los términos previstos en esta Ley Orgánica, así como las actividades preparatorias, no se considerarán intromisiones ilegítimas en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, a los efectos de lo establecido en el artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.

Artículo 16. *Instalación de sistemas fijos.*

1. En las vías o lugares públicos donde se instalen videocámaras fijas, el responsable del tratamiento deberá realizar una valoración del citado principio de proporcionalidad en su doble versión de idoneidad e intervención mínima. Asimismo, deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos relativo al tratamiento que se pretenda realizar, en función del nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida.

Se entenderá por videocámara fija aquella anclada a un soporte fijo o fachada, aunque el sistema de grabación se pueda mover en cualquier dirección.

2. Esta disposición se aplicará asimismo cuando las Fuerzas y Cuerpos de Seguridad utilicen instalaciones fijas de videocámaras de las que no sean titulares y exista, por su parte, un control y dirección efectiva del proceso completo de tratamiento.

3. Estas instalaciones fijas de videocámaras no estarán sujetas al control preventivo de las entidades locales previsto en su legislación reguladora básica, ni al ejercicio de las competencias de las diferentes Administraciones públicas, sin perjuicio de que deban respetar los principios de la legislación vigente en cada ámbito material de la actuación administrativa.

4. Los propietarios y, en su caso, los titulares de derechos reales sobre los bienes afectados por estas instalaciones, o quienes los posean por cualquier título, están obligados a facilitar y permitir su instalación y mantenimiento, sin perjuicio de las indemnizaciones que procedan.

5. Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos.

Artículo 17. *Dispositivos móviles.*

1. Podrán utilizarse dispositivos de toma de imágenes y sonido de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley Orgánica, conforme a las competencias específicas de las Fuerzas y Cuerpos de Seguridad. La toma de imagen y

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

sonido, que ha de ser conjunta, queda supeditada, en todo caso, a la concurrencia de un peligro o evento concreto. El uso de los dispositivos móviles deberá estar autorizado por la persona titular de la Delegación o Subdelegación del Gobierno, quien atenderá a la naturaleza de los eventuales hechos susceptibles de filmación, adecuando la utilización de dichos dispositivos a los principios de tratamiento y al de proporcionalidad.

En el caso de los Cuerpos de Policía propios de las Comunidades Autónomas que tengan y ejerzan competencias asumidas para la protección de las personas y bienes y para el mantenimiento del orden público, serán sus órganos correspondientes los que autorizarán este tipo de actuaciones para sus fuerzas policiales, así como para las dependientes de las Corporaciones locales radicadas en su territorio.

2. En estos supuestos de dispositivos móviles, las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro.

3. En casos de urgencia o necesidad inaplazable será el responsable operativo de las Fuerzas y Cuerpos de Seguridad competentes el que podrá determinar su uso, siendo comunicada tal actuación con la mayor brevedad posible, y siempre en el plazo de 24 horas, al Delegado o Subdelegado del Gobierno o autoridad competente de las comunidades autónomas.

Artículo 18. *Tratamiento y conservación de las imágenes.*

1. Realizada la filmación de acuerdo con los requisitos establecidos en esta Ley Orgánica, si la grabación captara la comisión de hechos que pudieran ser constitutivos de infracciones penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad, a disposición judicial a la mayor brevedad posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si se captaran hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad pública, se remitirán al órgano competente, de inmediato, para el inicio del oportuno procedimiento sancionador.

3. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto.

Artículo 19. *Régimen disciplinario.*

1. Sin perjuicio de las responsabilidades penales en las que pudieran incurrir, las infracciones a lo dispuesto en esta Ley Orgánica por los miembros de las Fuerzas y Cuerpos de Seguridad, serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de protección de datos de carácter personal establecido en esta Ley Orgánica.

2. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:

- a) Alterar o manipular los registros de imágenes y sonidos, siempre que no constituya delito.
- b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar estos para fines distintos de los previstos legalmente.
- c) Reproducir las imágenes y sonidos para fines distintos de los previstos en esta Ley Orgánica.
- d) Utilizar los medios técnicos regulados en esta Ley Orgánica para fines distintos de los previstos en la misma.

CAPÍTULO III

Derechos de las personas

Sección 1.ª Régimen general

Artículo 20. *Condiciones generales de ejercicio de los derechos de los interesados.*

1. El responsable del tratamiento deberá facilitar al interesado, de forma concisa, inteligible, de fácil acceso y con lenguaje claro y sencillo para todas las personas, incluidas aquellas con discapacidad, toda la información contemplada en el artículo 21, así como la derivada de los artículos 14, 22 a 26 y 39.

Además, el responsable del tratamiento deberá adoptar las medidas necesarias para garantizar al interesado el ejercicio de sus derechos a los que se refieren los artículos 14 y 22 a 26.

2. El interesado, con capacidad de obrar, podrá actuar en su propio nombre y representación o por medio de representantes, de acuerdo con lo previsto en la normativa sobre el procedimiento administrativo común de las Administraciones Públicas.

3. La información será facilitada por cualquier medio adecuado, incluidos los medios electrónicos, procurando utilizar el mismo medio empleado en la solicitud.

4. El responsable del tratamiento informará por escrito al interesado, sin dilación indebida, sobre el curso dado a su solicitud. La solicitud se entenderá desestimada si transcurrido un mes desde su presentación no ha sido resuelta expresamente y notificada al interesado.

5. La información a la que se refiere el apartado 1 se facilitará gratuitamente. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, en particular debido a su carácter repetitivo, el responsable del tratamiento podrá inadmitirlas a trámite, mediante resolución motivada.

El responsable del tratamiento deberá demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

En todo caso se considerará que la solicitud es repetitiva cuando se realicen tres solicitudes sobre el mismo supuesto durante el plazo de seis meses, salvo que exista causa legítima para ello.

6. Cuando el responsable del tratamiento tenga dudas razonables acerca de la identidad de la persona física que formula la solicitud a la que se refieren los artículos 22 y 23, le requerirá para que facilite la información complementaria que resulte necesaria para confirmar su identidad en el plazo de diez días. Transcurrido dicho plazo sin que se aporte la información, se le tendrá por desistido de su petición mediante resolución motivada. El plazo al que se refiere el apartado 4 comenzará a computarse desde la fecha en la que se facilite dicha información complementaria.

Artículo 21. *Información que debe ponerse a disposición del interesado.*

1. El responsable del tratamiento de los datos pondrá a disposición del interesado, al menos, la siguiente información:

- a) La identificación del responsable del tratamiento y sus datos de contacto.
- b) Los datos de contacto del delegado de protección de datos, en su caso.
- c) Los fines del tratamiento a los que se destinen los datos personales.
- d) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.
- e) El derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado y su rectificación, supresión o la limitación de su tratamiento.

2. Además de la información a la que se refiere el apartado 1, atendiendo a las circunstancias del caso concreto, el responsable del tratamiento proporcionará al interesado la siguiente información adicional para permitir el ejercicio de sus derechos:

- a) La base jurídica del tratamiento.
- b) El plazo durante el cual se conservarán los datos personales o, cuando esto no sea posible, los criterios utilizados para determinar ese plazo.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

c) Las categorías de destinatarios de los datos personales, cuando corresponda, en particular, los establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) Cualquier otra información necesaria, en especial, cuando los datos personales se hayan recogido sin conocimiento del interesado.

Artículo 22. *Derecho de acceso del interesado a sus datos personales.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen. En caso de que se confirme el tratamiento, el interesado tendrá derecho a acceder a dichos datos personales, así como a la siguiente información:

a) Los fines y la base jurídica del tratamiento.

b) Las categorías de datos personales de que se trate.

c) Los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular, los destinatarios establecidos en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.

d) El plazo de conservación de los datos personales, cuando sea posible, o, en caso contrario, los criterios utilizados para determinar dicho plazo.

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado o la limitación de su tratamiento.

f) El derecho a presentar una reclamación ante la autoridad de protección de datos competente y los datos de contacto de la misma.

g) La comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen, sin revelar la identidad de ninguna persona física, en especial en el caso de fuentes confidenciales.

2. Cuando el responsable trate una gran cantidad de información relativa al interesado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá requerir al interesado que concrete la solicitud en el plazo de diez días.

3. Se entenderá concedido el derecho de acceso si el responsable del tratamiento facilita al interesado un sistema remoto, directo y seguro que garantice, de modo permanente, el acceso a la totalidad de sus datos personales. La notificación informando al interesado del procedimiento puesto en marcha a través de este sistema, permitirá denegar su solicitud de acceso efectuada por otras vías.

Si el acceso remoto no facilita la totalidad de la información contenida en el apartado 1, el interesado tendrá derecho a solicitarla.

4. Cuando el interesado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho interesado asumirá el exceso de coste que su elección comporte. En este caso, sólo será exigible al responsable del tratamiento que la satisfacción del derecho de acceso a través del medio propuesto se produzca sin dilaciones indebidas. Si el interesado no asumiera el exceso de coste, se le facilitará el acceso por el medio inicialmente propuesto por el responsable del tratamiento.

Artículo 23. *Derechos de rectificación, supresión de datos personales y limitación de su tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento, sin dilación indebida, la rectificación de los datos personales que le conciernen, cuando tales datos resulten inexactos.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales cuando estos resulten incompletos.

El interesado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa del carácter incompleto o inexacto de los datos objeto de tratamiento.

2. El responsable del tratamiento, a iniciativa propia o como consecuencia del ejercicio del derecho de supresión del interesado, suprimirá los datos personales sin dilación indebida

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

y, en todo caso, en el plazo máximo de un mes a contar desde que tenga conocimiento, cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto.

3. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de los datos personales cuando se dé alguna de las siguientes circunstancias:

a) El interesado ponga en duda la exactitud de los datos personales y no pueda determinarse su exactitud o inexactitud.

b) Los datos personales hayan de conservarse a efectos probatorios.

Cuando el tratamiento esté limitado en virtud de la letra a), el responsable del tratamiento informará al interesado antes de levantar la limitación del tratamiento.

4. En caso de que el responsable del tratamiento rectifique unos datos personales inexactos que provengan de otra autoridad competente, se deberá comunicar a esta la rectificación.

5. Cuando los datos personales hayan sido rectificadas o suprimidos o el tratamiento haya sido limitado, el responsable del tratamiento lo notificará a los destinatarios, que deberán rectificar o suprimir los datos personales que estén bajo su responsabilidad o limitar su tratamiento.

Artículo 24. *Restricciones a los derechos de información, acceso, rectificación, supresión de datos personales y a la limitación de su tratamiento.*

1. El responsable del tratamiento podrá aplazar, limitar u omitir la información a la que se refiere el artículo 21.2, así como denegar, total o parcialmente, las solicitudes de ejercicio de los derechos contemplados en los artículos 22 y 23, siempre que, teniendo en cuenta los derechos fundamentales y los intereses legítimos de la persona afectada, resulte necesario y proporcional para la consecución de los siguientes fines:

a) Impedir que se obstaculicen indagaciones, investigaciones o procedimientos judiciales.

b) Evitar que se cause perjuicio a la prevención, detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.

c) Proteger la seguridad pública.

d) Proteger la Seguridad Nacional.

e) Proteger los derechos y libertades de otras personas.

2. En caso de restricción de los derechos contemplados en los artículos 22 y 23, el responsable del tratamiento informará por escrito al interesado sin dilación indebida, y en todo caso, en el plazo de un mes a contar desde que tenga conocimiento, de dicha restricción, de las razones de la misma, así como de las posibilidades de presentar una reclamación ante la autoridad de protección de datos, sin perjuicio de las restantes acciones judiciales que pueda ejercer en virtud de lo dispuesto en esta Ley Orgánica.

Las razones de la restricción podrán ser omitidas o ser sustituidas por una redacción neutra cuando la revelación de los motivos de la restricción pueda poner en riesgo los fines a los que se refiere el apartado anterior.

3. El responsable del tratamiento documentará los fundamentos de hecho o de derecho en los que se sustente la decisión denegatoria del ejercicio del derecho de acceso. Dicha información estará a disposición de las autoridades de protección de datos.

Artículo 25. *Ejercicio de los derechos del interesado a través de la autoridad de protección de datos.*

1. En los casos en que se produzca un aplazamiento, limitación u omisión de la información a que se refiere el artículo 21 o una restricción del ejercicio de los derechos contemplados en los artículos 22 y 23, en los términos previstos en el artículo 24, el interesado podrá ejercer sus derechos a través de la autoridad de protección de datos competente. El responsable del tratamiento informará al interesado de esta posibilidad.

2. Cuando, en virtud de lo establecido en el apartado anterior, se ejerciten los derechos a través de la autoridad de protección de datos, esta deberá informar al interesado, al menos,

de la realización de todas las comprobaciones necesarias o la revisión correspondiente y de su derecho a interponer recurso contencioso-administrativo.

Sección 2.ª Régimen especial

Artículo 26. *Derechos de los interesados como consecuencia de investigaciones y procesos penales.*

1. El ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales.

2. Cuando los datos sean objeto de un tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, en las normas procesales y en su caso, el Estatuto Orgánico del Ministerio Fiscal.

3. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica.

CAPÍTULO IV

Responsable y encargado de tratamiento

Sección 1.ª Obligaciones generales

Artículo 27. *Obligaciones del responsable del tratamiento.*

1. El responsable del tratamiento, tomando en consideración la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se lleve a cabo de acuerdo con esta Ley Orgánica y con lo previsto en la legislación sectorial y en sus normas de desarrollo. Tales medidas se revisarán y actualizarán cuando resulte necesario.

2. Entre las medidas mencionadas en el apartado anterior se incluirá la aplicación de las oportunas políticas de protección de datos, cuando sean proporcionadas en relación con las actividades de tratamiento.

Artículo 28. *Protección de datos desde el diseño y por defecto.*

1. En el momento de determinar los medios para el tratamiento, así como en el momento del tratamiento propiamente dicho, deberán aplicarse las medidas técnicas y organizativas que resulten apropiadas conforme al estado de la técnica y el coste de la aplicación, la naturaleza, el ámbito, el contexto, los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas. El objetivo será salvaguardar los principios de protección de datos de forma efectiva, al tiempo que integrar las garantías necesarias en el tratamiento. Entre estas medidas técnicas, se podrá adoptar la seudonimización de los datos personales a los efectos de contribuir a la aplicación de los principios establecidos en esta Ley Orgánica, en particular, el de minimización de datos personales.

2. Además, las medidas técnicas y organizativas deberán garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales que resulten necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad.

Tales medidas garantizarán que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas sin intervención humana.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

1. Cuando dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de tratamiento serán considerados corresponsables del tratamiento.

2. Salvo que las responsabilidades hayan sido previstas por el Derecho de la Unión Europea o por la legislación española, los corresponsables del tratamiento establecerán, de modo transparente y de mutuo acuerdo, a través del instrumento oportuno, sus respectivas responsabilidades en el cumplimiento de esta Ley Orgánica, en particular, en lo referido al ejercicio de los derechos del interesado y a sus respectivas obligaciones en el suministro de la información contemplada en el artículo 21.

El citado acuerdo designará el punto de contacto para los interesados, a menos que venga ya determinado legalmente.

La concreción de las responsabilidades se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Encargado del tratamiento.*

1. Cuando una operación de tratamiento vaya a ser llevada a cabo por cuenta de un responsable del tratamiento, este recurrirá únicamente a encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de esta Ley Orgánica y garantice la protección de los derechos del interesado.

El encargado podrá ser una persona física o jurídica, de naturaleza privada o pública.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito del responsable del tratamiento. El encargado informará siempre al responsable de cualquier cambio previsto referido a la adición o sustitución de otros encargados, pudiendo el responsable oponerse a dichos cambios.

3. El tratamiento por medio de un encargado se regirá por un contrato, convenio u otro instrumento jurídico que corresponda, por escrito, incluyendo la posibilidad del formato electrónico, concluido con arreglo al Derecho de la Unión Europea o a la legislación española. Dicho instrumento jurídico vinculará al encargado con el responsable y fijará el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable.

El instrumento jurídico estipulará, en particular, que el encargado del tratamiento deberá:

- a) Actuar únicamente siguiendo las instrucciones del responsable del tratamiento.
- b) Garantizar, a través del instrumento o sistema oportuno, que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de secreto o confidencialidad.
- c) Asistir al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado.
- d) Suprimir o devolver, a elección del responsable del tratamiento, todos los datos personales al responsable del tratamiento, una vez finalice la prestación de los servicios de tratamiento, así como suprimir las copias existentes, a menos que el Derecho de la Unión Europea o la legislación española requieran la conservación de los datos personales.
- e) Poner a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de estas obligaciones.
- f) Respetar las condiciones indicadas en este apartado y en el apartado 2 para contratar a otro encargado del tratamiento.

4. Si un encargado del tratamiento determinase los fines y medios de dicho tratamiento, infringiendo esta Ley Orgánica, será considerado responsable con respecto a ese tratamiento.

5. El encargado del tratamiento se regirá, en lo no previsto por esta Ley Orgánica, por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 31. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento, así como cualquier persona que actúe bajo la autoridad del responsable o del encargado del tratamiento y tenga acceso a datos personales, sólo podrá

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

someterlos a tratamiento siguiendo instrucciones del responsable del tratamiento, a menos que esté obligado a hacerlo por el Derecho de la Unión Europea o por la legislación española.

Artículo 32. *Registros de las actividades de tratamiento.*

1. Cada responsable debe conservar un registro de todas las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad. Dicho registro deberá contener la información siguiente:

- a) La identificación del responsable del tratamiento y sus datos de contacto, así como, en su caso, del corresponsable y del delegado de protección de datos.
- b) Los fines del tratamiento.
- c) Las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en Estados que no sean miembros de la Unión Europea u organizaciones internacionales.
- d) La descripción de las categorías de interesados y de las categorías de datos personales.
- e) El recurso a la elaboración de perfiles, en su caso.
- f) Las categorías de transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso.
- g) La indicación de la base jurídica del tratamiento, así como, en su caso, las transferencias internacionales de las que van a ser objeto los datos personales.
- h) Los plazos previstos para la supresión de las diferentes categorías de datos personales, cuando sea posible.
- i) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

2. Cada encargado del tratamiento llevará un registro de todas las actividades de tratamiento de datos personales efectuadas en nombre de un responsable. Este registro contendrá la información siguiente:

- a) El nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, en su caso, del delegado de protección de datos.
- b) Las categorías de tratamientos efectuados en nombre de cada responsable.
- c) Las transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional, en su caso, incluida la identificación de dicho Estado o de dicha organización internacional cuando el responsable del tratamiento así lo ordene explícitamente.
- d) La descripción general de las medidas técnicas y organizativas de seguridad a las que se refiere el artículo 37.1, cuando sea posible.

3. Los registros referidos en este artículo se establecerán y llevarán por escrito, incluida la posibilidad del formato electrónico.

Estos registros estarán a disposición de la autoridad de protección de datos competente, a solicitud de esta, de conformidad con lo dispuesto legalmente.

4. Los responsables de los tratamientos harán público el registro de sus actividades de tratamiento, accesible por medios electrónicos, en el que constará la información a la que se refiere el apartado 1.

Artículo 33. *Registro de operaciones.*

1. Los responsables y encargados del tratamiento deberán mantener registros de, al menos, las siguientes operaciones de tratamiento en sistemas de tratamiento automatizados: recogida, alteración, consulta, comunicación, incluidas las transferencias, y combinación o supresión. Los registros de consulta y comunicación harán posible determinar la justificación, la fecha y la hora de tales operaciones y, en la medida de lo posible, el nombre de la persona que consultó o comunicó los datos personales, así como la identidad de los destinatarios de dichos datos personales.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

2. Estos registros se utilizarán únicamente a efectos de verificar la legalidad del tratamiento, controlar el cumplimiento de las medidas y de las políticas de protección de datos y garantizar la integridad y la seguridad de los datos personales en el ámbito de los procesos penales.

Dichos registros estarán a disposición de la autoridad de protección de datos competente a solicitud de esta, de conformidad con lo dispuesto legalmente.

Artículo 34. *Cooperación con las autoridades de protección de datos.*

El responsable y el encargado del tratamiento cooperarán con la autoridad de protección de datos competente, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones.

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, suponga por su naturaleza, alcance, contexto o fines, un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.

2. La evaluación incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos peligros, así como las medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar su conformidad con esta Ley Orgánica. Esta evaluación tendrá en cuenta los derechos e intereses legítimos de los interesados y de las demás personas afectadas.

3. Las autoridades de protección de datos podrán establecer una lista de tratamientos que estén sujetos a la realización de una evaluación de impacto con arreglo a lo dispuesto en el apartado anterior y, del mismo modo, podrán establecer una lista de tratamientos que no estén sujetos a esta obligación. Ambas listas tendrán un carácter meramente orientativo.

Artículo 36. *Consulta previa a la autoridad de protección de datos.*

1. El responsable o el encargado del tratamiento consultará a la autoridad de protección de datos, antes de proceder al tratamiento de datos personales que vayan a formar parte de un nuevo fichero, en cualquiera de las siguientes circunstancias:

a) Cuando la evaluación del impacto en la protección de los datos indique que el tratamiento entrañaría un alto nivel de riesgo, a falta de medidas adoptadas por el responsable para mitigar el riesgo o los posibles daños.

b) Cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos.

2. La autoridad de protección de datos correspondiente podrá establecer una lista de carácter orientativo, de las operaciones de tratamiento sujetas a consulta previa, con arreglo a lo dispuesto en el apartado anterior.

3. El responsable del tratamiento facilitará a la autoridad de protección de datos competente, la evaluación de impacto contemplada en el artículo 35 y, previa solicitud, cualquier información adicional que permita a dicha autoridad de protección de datos evaluar la conformidad del tratamiento y, más concretamente, el nivel de riesgo para la protección de los datos personales del interesado y las garantías correspondientes.

4. Cuando la autoridad de protección de datos considere que el tratamiento previsto en el apartado 1 pudiera infringir lo dispuesto en esta Ley Orgánica deberá, en un plazo de seis semanas desde la solicitud de la consulta, asesorar por escrito al responsable del tratamiento y, en su caso, al encargado del tratamiento, en especial, cuando el responsable del tratamiento no haya identificado o mitigado suficientemente el peligro o el nivel de riesgo. Asimismo, la autoridad de protección de datos podrá ejercer cualquiera de sus potestades de investigación, corrección o consulta.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

Este plazo podrá prorrogarse un mes, en función de la complejidad del tratamiento previsto. La autoridad de protección de datos informará al responsable y, en su caso, al encargado acerca de la prórroga, en el plazo de un mes a partir de la recepción de la solicitud de consulta, junto con los motivos de la dilación.

En caso de no contestar a la consulta en el plazo previsto, no operará la presunción del carácter favorable del mismo.

Sección 2.ª Seguridad de los datos personales

Artículo 37. Seguridad del tratamiento.

1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.

2. Por lo que respecta al tratamiento automatizado, el responsable o encargado del tratamiento, a raíz de una evaluación de los riesgos, pondrá en práctica medidas de control con el siguiente propósito:

a) En el control de acceso a los equipamientos, denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento.

b) En el control de los soportes de datos, impedir que estos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas.

c) En el control del almacenamiento, impedir que se introduzcan sin autorización datos personales, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización.

d) En el control de los usuarios, impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos.

e) En el control del acceso a los datos, garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado, sólo puedan tener acceso a los datos personales para los que han sido autorizados.

f) En el control de la transmisión, garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse, o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos.

g) En el control de la introducción, garantizar que pueda verificarse y constatarse, a posteriori, qué datos personales se han introducido en los sistemas de tratamiento automatizado, en qué momento y quién los ha introducido.

h) En el control del transporte, impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización.

i) En el control de restablecimiento, garantizar que los sistemas instalados puedan restablecerse en caso de interrupción.

j) En el control de fiabilidad e integridad, garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema.

Artículo 38. Notificación a la autoridad de protección de datos de una violación de la seguridad de los datos personales.

1. Cualquier violación de la seguridad de los datos personales será notificada por el responsable del tratamiento a la autoridad de protección de datos competente, a menos que sea improbable que la violación de la seguridad de los datos personales constituya un peligro para los derechos y las libertades de las personas físicas.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

La notificación deberá realizarse en el plazo de las setenta y dos horas siguientes al momento en que se haya tenido constancia de ella. En caso contrario, deberá ir acompañada de los motivos de la dilación.

2. El encargado del tratamiento notificará, sin dilación indebida, al responsable del tratamiento, las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, al menos:

a) Referir la naturaleza de la violación de la seguridad de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de personas afectadas, así como las categorías y el número aproximado de registros de datos personales afectados por la violación de la seguridad.

b) Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Detallar las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar sus posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, se podrá facilitar de forma progresiva, a medida que se disponga de ella.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relativos a dicha violación, sus efectos y las medidas correctivas adoptadas.

Dicha documentación estará a disposición de la autoridad de protección de datos competente al objeto de verificar el cumplimiento de lo dispuesto en este artículo.

6. Cuando la violación de la seguridad de los datos personales afecte a datos que hayan sido transmitidos por el responsable del tratamiento o al responsable del tratamiento de otro Estado miembro de la Unión Europea, la información recogida en el apartado 3 se comunicará al responsable del tratamiento de dicho Estado.

7. Todas las actividades relacionadas en este artículo se realizarán sin dilaciones indebidas.

Artículo 39. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando existan indicios de que una violación de la seguridad de los datos personales supondría un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento comunicará al interesado, sin dilación indebida, la violación de la seguridad de los datos personales.

2. La comunicación al interesado describirá con lenguaje claro, sencillo y accesible conforme a sus circunstancias y capacidades, la naturaleza de la violación de la seguridad de los datos personales y contendrá, al menos, la información y las medidas a las que se refiere el artículo 38.3. b), c) y d).

3. No se efectuará la comunicación al interesado que prevé el apartado 1 cuando se cumpla alguna de las condiciones siguientes:

a) Que el responsable del tratamiento haya adoptado medidas apropiadas de protección técnica y organizativa y dichas medidas se hayan aplicado a los datos personales afectados por la violación de la seguridad antes de la misma, en particular, aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como en el caso del cifrado.

b) Que el responsable del tratamiento haya tomado medidas ulteriores para garantizar que no se materialice el alto nivel de riesgo para los derechos y libertades del interesado a que hace referencia el apartado 1.

c) Que suponga un esfuerzo desproporcionado, en cuyo caso, se optará por su publicación en el boletín oficial correspondiente, en la sede electrónica del responsable del tratamiento o en otro canal oficial que permita una comunicación efectiva con el interesado.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

4. En el supuesto de que el responsable del tratamiento no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de protección de datos competente, una vez valorada la existencia de un alto nivel de riesgo, podrá exigirle que proceda a dicha comunicación, o bien que determine la concurrencia de alguna de las condiciones previstas en el apartado 3.

5. La comunicación al interesado referida en el apartado 1 podrá aplazarse, limitarse u omitirse con sujeción a las condiciones y por los motivos previstos en el artículo 24.

Sección 3.ª Delegado de protección de datos

Artículo 40. *Designación del delegado de protección de datos.*

1. Los responsables del tratamiento designarán, en todo caso, un delegado de protección de datos. No estarán obligados a designarlo los órganos jurisdiccionales o el Ministerio Fiscal cuando el tratamiento de datos personales se realice en el ejercicio de sus funciones jurisdiccionales.

2. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales. En concreto, se tendrán en cuenta sus conocimientos especializados en legislación, su experiencia en materia de protección de datos y su capacidad para desempeñar las funciones a las que se refiere el artículo 42. En el caso de haber designado un delegado de protección de datos al amparo del Reglamento General de Protección de Datos, este será el que asumirá las funciones de delegado de protección de datos previstas en esta Ley Orgánica.

3. Podrá designarse a un único delegado de protección de datos para varias autoridades competentes, teniendo en cuenta la estructura organizativa y el tamaño de estas.

4. Los responsables del tratamiento publicarán los datos de contacto del delegado de protección de datos y comunicarán a la autoridad de protección de datos competente su designación y cese, en el plazo de diez días desde que se haya producido.

Artículo 41. *Posición del delegado de protección de datos.*

1. El responsable del tratamiento velará porque el delegado de protección de datos participe adecuada y oportunamente en todas las cuestiones relativas a la protección de datos personales, al tiempo que cuidará de que mantenga sus conocimientos especializados, cuente con los recursos necesarios para el desempeño de sus funciones y acceda a los datos personales y a las operaciones de tratamiento.

2. El delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitar cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento. La existencia de cualquier deber de confidencialidad o secreto no permitirá que el responsable o el encargado del tratamiento se oponga a dicho acceso.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de dirección del responsable o del encargado del tratamiento.

Artículo 42. *Funciones del delegado de protección de datos.*

El responsable del tratamiento encomendará al delegado de protección de datos, al menos, las siguientes funciones:

a) Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo, acerca de las obligaciones que les incumben en virtud de esta Ley Orgánica y de otras disposiciones de protección de datos aplicables.

b) Supervisar el cumplimiento de lo dispuesto en esta Ley Orgánica y en otras disposiciones de protección de datos aplicables, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales, incluidas la

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

asignación de responsabilidades, la concienciación y formación del personal que participe en las operaciones de tratamiento y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización.

d) Cooperar con la autoridad de protección de datos en los términos de la legislación vigente.

e) Actuar como punto de contacto de la autoridad de protección de datos para las cuestiones relacionadas con el tratamiento, incluida la consulta previa referida en el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

CAPÍTULO V

Transferencias de datos personales a terceros países que no sean miembros de la Unión Europea o a organizaciones internacionales

Artículo 43. *Principios generales de las transferencias de datos personales.*

1. Al objeto de garantizar el nivel de protección de las personas físicas previsto en esta Ley Orgánica, cualquier transferencia de datos personales realizada por las autoridades competentes españolas a un Estado que no sea miembro de la Unión Europea o a una organización internacional, incluidas las transferencias ulteriores a otro Estado que no pertenezca a la Unión Europea o a otra organización internacional, deberá cumplir las siguientes condiciones:

a) Que la transferencia sea necesaria para los fines establecidos en el artículo 1.

b) Que los datos personales sean transferidos a un responsable del tratamiento competente para los fines mencionados en el artículo 1.

c) Que, en caso de que los datos personales hayan sido transferidos a la autoridad competente española procedentes de otro Estado miembro de la Unión Europea, dicho Estado miembro autorice previamente la transferencia ulterior de conformidad con su Derecho nacional.

d) Que la Comisión Europea haya adoptado una decisión de adecuación de acuerdo con el artículo 44 o, a falta de dicha decisión, cuando se hayan aportado o existan garantías apropiadas de conformidad con el artículo 45 o, a falta de ambas, cuando resulten de aplicación las excepciones para situaciones específicas de acuerdo con el artículo 46.

e) Cuando se trate de una transferencia ulterior a un Estado que no sea miembro de la Unión Europea u organización internacional, de datos transferidos inicialmente por una autoridad competente española, esta autorizará la transferencia ulterior, una vez considerados todos los factores pertinentes, entre estos, la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección existente en ese Estado u organización internacional a los que se transfieran ulteriormente los datos personales.

2. Las transferencias de datos personales por las autoridades españolas sin autorización previa de otro Estado miembro, conforme al párrafo 1c), sólo se permitirán si la transferencia de datos personales resulta necesaria para prevenir una amenaza inmediata y grave para la seguridad pública, tanto de un Estado miembro de la Unión Europea como no perteneciente a la misma, o para los intereses fundamentales de un Estado miembro de la Unión Europea, y cuando la autorización previa no pueda conseguirse a su debido tiempo.

Las autoridades españolas informarán sin dilación a la autoridad responsable de conceder la autorización previa, y en todo caso en el plazo máximo de diez días a contar desde que se haya producido la transferencia.

3. Se impulsará el establecimiento de mecanismos de cooperación internacional y de asistencia mutua y se fomentará el intercambio de normativa y de buenas prácticas con los Estados que no sean miembros de la Unión Europea y con las organizaciones internacionales, de manera que se facilite la aplicación efectiva de la legislación sobre la protección de datos personales, inclusive en el ámbito de la resolución de conflictos jurisdiccionales, procurando la participación de todas las partes interesadas.

Artículo 44. *Transferencias basadas en una decisión de adecuación.*

1. Cuando la Comisión Europea, mediante una decisión de adecuación, haya decidido que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o la organización internacional de que se trate, garantizan un nivel de protección adecuado, podrán realizarse transferencias de datos personales a ese Estado u organización internacional. Dichas transferencias no requerirán ninguna autorización específica.

2. Toda decisión de adecuación de la Comisión Europea que determine que un Estado que no sea miembro de la Unión Europea, un territorio o uno o varios sectores específicos de dicho Estado, o una organización internacional ha dejado de garantizar un nivel de protección adecuado, se entenderá sin perjuicio de las transferencias de datos personales a dicho Estado, territorio o sector del mismo o a la organización internacional de que se trate, en virtud de los artículos 45 y 46.

Artículo 45. *Transferencias mediante garantías apropiadas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea conforme al artículo 44 podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando concorra alguna de las siguientes circunstancias:

a) Se hayan aportado garantías apropiadas respecto a la protección de datos personales en un instrumento jurídicamente vinculante.

b) Se hayan evaluado, por parte del responsable del tratamiento, todas las circunstancias que concurren en la transferencia de datos personales y se haya concluido que existen garantías apropiadas respecto a la protección de datos personales.

2. El responsable del tratamiento informará a la autoridad de protección de datos competente acerca de las categorías de transferencias a tenor del párrafo 1.b).

3. Cuando las transferencias se basen en lo dispuesto en el párrafo 1.b) deberán documentarse. La documentación se pondrá a disposición de la autoridad de protección de datos competente, previa solicitud, con inclusión de la siguiente información: fecha, hora de la transferencia, información sobre la autoridad competente destinataria, justificación de la transferencia y datos personales transferidos.

Artículo 46. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de la Comisión Europea o de garantías apropiadas de acuerdo con los artículos 44 y 45, podrán realizarse transferencias de datos personales a un Estado que no sea miembro de la Unión Europea o a una organización internacional cuando la transferencia sea necesaria por concurrir alguna de las siguientes circunstancias:

a) Para proteger los intereses vitales o los derechos y libertades fundamentales del interesado o de otra persona.

b) Para salvaguardar intereses legítimos del interesado reconocidos por la legislación española.

c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado, tanto miembro de la Unión Europea como no perteneciente a la misma.

d) En casos individuales, a efectos del artículo 1.

e) Para el ejercicio, en un caso individual, de acciones legales o para la defensa frente a ellas en relación con los fines incluidos en el artículo 1.

2. Los datos personales no se transferirán, si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público en la transferencia, establecido en las letras d) y e) del apartado anterior.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse. Esta documentación quedará a disposición de la autoridad de protección de datos competente, con inclusión de la fecha y la hora de la transferencia, la información sobre la

autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

Artículo 47. *Transferencias directas de datos personales a destinatarios, que no sean autoridades competentes, establecidos en Estados no pertenecientes a la Unión Europea.*

1. Excepcionalmente, en casos particulares y específicos y sin perjuicio de la existencia de un acuerdo internacional entre España y un Estado que no sea miembro de la Unión Europea en el ámbito de la cooperación judicial penal o de la cooperación policial, las autoridades competentes españolas podrán transferir datos personales directamente a destinatarios que no tengan la condición de autoridad competente, establecidos en Estados que no sean miembros de la Unión Europea, siempre que se cumplan las disposiciones de esta Ley Orgánica y se satisfagan todas las condiciones siguientes:

a) Que la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente que lleva a cabo la transferencia conforme al Derecho de la Unión Europea o a la legislación española, con cualquiera de los fines del artículo 1.

b) Que la autoridad competente que realiza la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado son superiores al interés público que precise de la transferencia de que se trate.

c) Que la autoridad competente que realiza la transferencia considere que la transferencia a una autoridad competente del Estado en el que está establecido el destinatario, con cualquiera de los fines del artículo 1, resultaría ineficaz o inadecuada, en particular porque la transferencia no pueda efectuarse dentro de plazo.

d) Que se informe sin dilación indebida a la autoridad competente para los fines que contempla el artículo 1 de dicho Estado, salvo que esto resulte ineficaz o inadecuado.

e) Que la autoridad competente que realiza la transferencia informe al destinatario de la finalidad o finalidades específicas para las que puede tratar los datos personales, siempre y cuando dicho tratamiento sea necesario.

2. La autoridad competente que realiza la transferencia informará a la autoridad de protección de datos competente acerca de las transferencias efectuadas a tenor de este artículo.

3. Las transferencias basadas en lo dispuesto en este artículo deberán documentarse.

CAPÍTULO VI

Autoridades de Protección de Datos Independientes

Artículo 48. *Autoridades de protección de datos.*

A los efectos de esta Ley Orgánica son autoridades de protección de datos independientes:

a) La Agencia Española de Protección de Datos.

b) Las autoridades autonómicas de protección de datos, exclusivamente en relación a aquellos tratamientos de los que sean responsables en su ámbito de competencia, y conforme a lo dispuesto en el artículo 57.1 de la Ley Orgánica 3/2018, de 5 de diciembre, y en la normativa autonómica aplicable.

Dichas autoridades se regirán por esta Ley Orgánica respecto de los tratamientos sometidos a la misma, de acuerdo con los principios de cooperación institucional, coordinación de criterios e información mutua, y por lo establecido en el Título VII de la Ley Orgánica 3/2018, de 5 de diciembre, y en sus normas de creación, así como por lo que establezcan sus normas de desarrollo.

La Agencia Española de Protección de Datos actuará como representante de las autoridades de protección de datos en el Comité Europeo de Protección de Datos.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

Artículo 49. Funciones.

1. Las autoridades de protección de datos ejercerán, respecto de los tratamientos sometidos a esta Ley Orgánica, las siguientes funciones:

a) Supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta Ley Orgánica.

b) Promover la sensibilización y la comprensión de la ciudadanía acerca de los riesgos, normas, garantías y derechos relativos al tratamiento.

c) Asesorar a las Cortes Generales, al Gobierno de la Nación y a los organismos dependientes o vinculados a la Administración General del Estado, así como, de acuerdo con su ámbito competencial, a las Asambleas Legislativas de las comunidades autónomas, los Consejos de Gobierno y los organismos dependientes o vinculados a la Administración de las comunidades autónomas, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento.

d) Promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben.

e) Facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta Ley Orgánica y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

f) Tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable.

g) Controlar, de acuerdo con lo dispuesto en el artículo 25, la licitud del tratamiento e informar al interesado en un plazo razonable sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo.

h) Cooperar, en particular compartiendo información, con otras autoridades de protección de datos y prestarse asistencia mutua.

i) Llevar a cabo investigaciones sobre la aplicación de esta Ley Orgánica, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública.

j) Realizar un seguimiento de acontecimientos que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, de manera concreta sobre el desarrollo de las tecnologías de la información y la comunicación.

k) Prestar asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36.

l) Contribuir a las actividades del Comité Europeo de Protección de Datos.

m) Informar todas las disposiciones legales o reglamentarias que afecten a tratamientos sometidos a esta Ley Orgánica.

2. Las autoridades de protección de datos adoptarán medidas tendentes a facilitar la formulación de las reclamaciones incluidas en el párrafo 1f), tales como proporcionar formularios que puedan cumplimentarse electrónicamente, sin excluir otros medios.

3. El desempeño de las funciones de las autoridades de control no implicará coste alguno para el interesado ni para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de protección de datos podrá negarse a actuar respecto de la solicitud. La carga de la demostración del carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de protección de datos.

Artículo 50. Potestades.

Las autoridades de protección de datos tendrán atribuidas, en el ámbito de esta Ley Orgánica, las siguientes potestades:

a) De investigación, incluyendo el acceso a todos los datos que estén siendo tratados por el responsable o el encargado del tratamiento, en los términos previstos por la legislación vigente.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

b) De advertencia y control de lo exigido en esta Ley Orgánica, incluida la sanción de las infracciones cometidas, la elaboración de recomendaciones, órdenes de rectificación, supresión o limitación del tratamiento de datos personales o de limitación temporal o definitiva del tratamiento, incluida su prohibición, así como la orden a los responsables del tratamiento de comunicar las vulneraciones de seguridad de los datos a los interesados.

c) De asesoramiento, que comprende la consulta previa prevista en el artículo 36 y la emisión, por propia iniciativa o previa solicitud, de dictámenes destinados a las Cortes Generales o al Gobierno, a otras instituciones u organismos, así como al público en general, acerca de todo asunto relacionado con la protección de datos personales sujeto a esta Ley Orgánica.

Artículo 51. *Asistencia entre autoridades de protección de datos de los Estados miembros de la Unión Europea.*

1. Las autoridades de protección de datos españolas facilitarán la asistencia y cooperación necesaria a las autoridades de protección de datos de otros Estados miembros de la Unión Europea, debiendo responder a las solicitudes de estas sin dilación indebida, y en cualquier caso, en el plazo máximo de un mes desde su recepción. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, así como las solicitudes para llevar a cabo consultas, inspecciones e investigaciones.

2. Las autoridades de protección de datos españolas podrán solicitar, en el ejercicio de sus funciones, la asistencia y cooperación de las autoridades de protección de datos de otros Estados miembros de la Unión Europea.

Las solicitudes deberán contener toda la información necesaria para su contestación, incluidos los motivos y la finalidad de la solicitud. La información intercambiada se utilizará únicamente para el fin para el que haya sido solicitada.

3. Las contestaciones de las autoridades de protección de datos españolas deberán indicar los resultados obtenidos o las medidas adoptadas con base en la solicitud recibida. Estas respuestas serán remitidas en formato electrónico, en la medida de lo posible.

4. La solicitud de asistencia procedente de una autoridad de protección de datos de un Estado miembro de la Unión Europea únicamente podrá negarse a ser atendida, de manera motivada, cuando la autoridad de protección de datos española no sea competente respecto al objeto o a las medidas solicitadas, o bien cuando el hecho de atender la solicitud vulnere la legislación española o el Derecho de la Unión Europea. Se informará, en su caso, de la restricción de los derechos del interesado adoptada en aplicación del artículo 24.

5. Las medidas adoptadas con ocasión de una solicitud de asistencia mutua serán gratuitas, sin perjuicio de que en circunstancias excepcionales puedan pactarse indemnizaciones por gastos específicos derivados de la prestación de la asistencia.

CAPÍTULO VII

Reclamaciones

Artículo 52. *Régimen aplicable a los procedimientos tramitados ante las autoridades de protección de datos.*

1. En el caso de que los interesados aprecien que el tratamiento de los datos personales haya infringido las disposiciones de esta Ley Orgánica o no haya sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 21, 22 y 23 tendrán derecho a presentar una reclamación ante la autoridad de protección de datos.

2. Dichas reclamaciones serán tramitadas por la autoridad de protección de datos competente con sujeción al procedimiento establecido en el título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, y, en su caso, a la legislación de las Comunidades Autónomas que resulte de aplicación. Tendrán carácter subsidiario las normas generales sobre los procedimientos administrativos y el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

4. Sin perjuicio de lo dispuesto en el artículo 55, todo interesado tendrá derecho a interponer recurso contencioso-administrativo, de acuerdo con su normativa reguladora, en caso de que la autoridad de protección de datos competente no dicte resolución expresa y se la notifique en el plazo de tres meses.

Artículo 53. *Derecho a indemnización por entes del sector público.*

1. Los interesados tendrán derecho a ser indemnizados por el responsable del tratamiento, o por el encargado del tratamiento cuando formen parte del sector público, en el caso de que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica.

2. Cuando quien incumpla lo dispuesto en esta Ley Orgánica tenga la consideración de Administración pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad patrimonial previsto en la normativa sobre el procedimiento administrativo común de las Administraciones públicas y sobre el régimen jurídico del sector público.

3. En el caso de que la actuación provenga de un órgano judicial o del Ministerio Fiscal cuando se realice el tratamiento con fines jurisdiccionales la responsabilidad se regirá por lo dispuesto en el Título V del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Artículo 54. *Derecho a indemnización por encargados del tratamiento del sector privado.*

1. Los interesados que sufran daño o lesión en sus bienes o derechos por parte del encargado del tratamiento que no forme parte del sector público, como consecuencia del incumplimiento de lo dispuesto en esta Ley Orgánica, tendrán derecho a ser indemnizados.

2. El encargado del tratamiento estará obligado a indemnizar todos los daños y perjuicios que cause a los interesados o a terceros como resultado de las operaciones de tratamientos de datos previstas en el contrato u otro instrumento o acto jurídico suscrito con el responsable del tratamiento conforme al artículo 30, de conformidad con el régimen de responsabilidad del contratista por los daños causados a terceros regulado en la normativa sobre contratos del sector público.

3. Cuando tales daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la autoridad competente responsable del tratamiento, será esta la responsable.

4. Los interesados o los terceros perjudicados podrán requerir al responsable del tratamiento, dentro del año siguiente a la producción del hecho, para que informe, una vez oído el encargado del tratamiento, acerca de a cuál de las partes contratantes o de las que hayan suscrito el acto jurídico conforme al artículo 30, corresponde la responsabilidad de los daños. El ejercicio de esta facultad interrumpe el plazo de prescripción de la acción.

5. Con independencia de lo previsto en los apartados anteriores, el encargado del tratamiento que no forme parte del sector público responderá de los daños y perjuicios que durante las operaciones de tratamiento de datos cause. Deberá hacerlo tanto respecto del responsable del tratamiento, como respecto del interesado o de terceros por incumplimientos de esta Ley Orgánica, de infracciones de preceptos legales o reglamentarios, o por el incumplimiento de las previsiones contenidas en el contrato o en otro acto jurídico suscrito. El encargado del tratamiento que no forme parte del sector público deberá haber incurrido en actuaciones que le sean imputables, sin perjuicio de la aplicación del régimen sancionador, en su caso.

Artículo 55. *Tutela judicial efectiva.*

1. Sin perjuicio de cualquier otro recurso administrativo o reclamación, toda persona física o jurídica tendrá derecho a recurrir ante la jurisdicción contencioso-administrativa, de acuerdo con su legislación reguladora, contra los actos y resoluciones dictadas por la autoridad de protección de datos competente.

2. El interesado podrá conferir su representación a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los

derechos y libertades de los interesados en materia de protección de sus datos personales, para que ejerza los derechos contemplados en el apartado anterior.

CAPÍTULO VIII

Régimen sancionador

Artículo 56. *Sujetos responsables.*

1. La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción.

2. Están sujetos al régimen sancionador:

- a) Los responsables de los tratamientos.
- b) Los encargados de los tratamientos.
- c) Los representantes de los encargados no establecidos en el territorio de la Unión Europea.
- d) El resto de las personas físicas o jurídicas obligadas por el contenido del deber de colaboración establecido en el artículo 7.

3. No será de aplicación el régimen sancionador establecido en este capítulo al delegado de protección de datos.

Artículo 57. *Concurso de normas.*

1. Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra Ley, siempre que no constituyan infracciones al Reglamento General de Protección de Datos, ni a la Ley Orgánica 3/2018, de 5 de diciembre, se sancionarán observando las siguientes reglas:

- a) El precepto especial se aplicará con preferencia al general.
- b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.
- c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción que conlleve una mayor sanción.

Artículo 58. *Infracciones muy graves.*

Son infracciones muy graves:

a) El tratamiento de datos personales que vulnere los principios y garantías establecidos en el artículo 6 o sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 11, siempre que se causen perjuicios de carácter muy grave a los interesados.

b) El acceso, cesión, alteración y divulgación de los datos al margen de los supuestos autorizados por el responsable o encargado de los datos, siempre que no constituya ilícito penal.

c) La transferencia temporal o definitiva de datos de carácter personal con destino a Estados que no sean miembros de la Unión Europea o a destinatarios que no sean autoridades competentes, establecidos en dichos Estados incumpliendo las condiciones previstas en los artículos 43 y 47.

d) La utilización de los datos para una finalidad que no sea compatible con el objetivo para el que fueron recogidos o cuando no se cumplan las condiciones establecidas en el artículo 6, siempre que no se cuente con una base legal para ello.

e) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, que cause perjuicios graves a los interesados.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

f) La omisión del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en esta Ley Orgánica.

g) La vulneración del deber de confidencialidad del encargado del tratamiento, establecido en el artículo 30.

h) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que se causen perjuicios de carácter muy grave para los interesados.

i) El impedimento, la obstaculización o la falta de atención reiterada del ejercicio de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que se causen perjuicios de carácter muy grave para los interesados.

j) La negativa a proporcionar a las autoridades competentes la información necesaria para la prevención, detección, investigación y enjuiciamiento de infracciones penales, para la ejecución de sanciones penales o para la protección y prevención frente a las amenazas contra la seguridad pública de acuerdo con lo previsto en el artículo 7, así como a informar al interesado cuando se comuniquen sus datos en virtud del deber de colaboración establecido en dicho artículo.

k) La resistencia u obstrucción del ejercicio de la función inspectora de las autoridades de protección de datos competentes.

l) La falta de notificación a las autoridades de protección de datos competentes acerca de una violación de la seguridad de los datos personales, cuando sea exigible, así como la ausencia de comunicación al interesado de una violación de la seguridad cuando sea procedente de acuerdo con el artículo 39, siempre que se deriven perjuicios de carácter muy grave para el interesado.

m) El incumplimiento de las resoluciones dictadas por las autoridades de protección de datos competentes, en el ejercicio de las potestades que le confiere el artículo 50.

n) No facilitar el acceso del personal de las autoridades de protección de datos competentes a los datos personales, información, locales, equipos y medios de tratamiento, cuando sean requeridos por las mismas, en el ejercicio de sus poderes de investigación.

ñ) El incumplimiento de los plazos de conservación y revisión establecidos en virtud del artículo 8.

Artículo 59. Infracciones graves.

Son infracciones graves:

a) El tratamiento de los datos de carácter personal cuando se incumplan los principios del artículo 6 o las condiciones de licitud del tratamiento del artículo 11, siempre que no constituya una infracción muy grave.

b) El tratamiento de datos personales de las categorías especiales sin que concurra alguna de las circunstancias previstas en el artículo 13 o sin garantizar las medidas de seguridad adecuadas, siempre que no constituya una infracción muy grave.

c) La adopción de decisiones individuales automatizadas sin las garantías señaladas en el artículo 14, siempre que no constituya una infracción muy grave.

d) La falta de designación de un delegado de protección de datos en los términos previstos en el artículo 40 o no posibilitar la efectiva participación del mismo en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

e) El incumplimiento de la puesta a disposición al interesado de la información prevista en el artículo 21 o del deber de comunicación al mismo, o a la autoridad de protección de datos competente, de una violación de la seguridad de los datos, que entrañe un grave perjuicio para los derechos y libertades del interesado.

f) La ausencia de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos, incluidas las medidas oportunas desde el diseño y por defecto, así como para integrar las garantías necesarias en el tratamiento.

g) El impedimento, la falta de atención o la obstaculización de los derechos del interesado de acceso, rectificación, supresión de sus datos o limitación del tratamiento, siempre que no constituya infracción muy grave.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

h) El incumplimiento de la obligación de llevanza de los registros de actividades de tratamiento o del registro de operaciones de tratamiento, si se causan perjuicios de carácter grave a los interesados.

i) El incumplimiento de las estipulaciones recogidas en el contrato u acto jurídico que vincula al responsable y al encargado del tratamiento, salvo en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento, así como el incumplimiento de las obligaciones impuestas en el artículo 30.

j) La falta de colaboración diligente con las autoridades competentes en el cumplimiento de las obligaciones establecidas en el artículo 7, cuando no constituya una infracción muy grave.

k) La falta de cooperación, la actuación negligente o el impedimento de la función inspectora de las autoridades de protección de datos competentes, cuando no constituya infracción muy grave.

l) El incumplimiento de la evaluación de impacto en la protección de los datos de carácter personal, si se derivan perjuicios o riesgos de carácter grave para los interesados.

m) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos competente, en los casos en que dicha consulta resulte preceptiva conforme al artículo 36.

Artículo 60. Infracciones leves.

Son infracciones leves:

a) La afectación leve de los derechos de los interesados como consecuencia de la ausencia de la debida diligencia o del carácter inadecuado o insuficiente de las medidas técnicas y organizativas que se hubiesen implantado.

b) El incumplimiento del principio de transparencia de la información o del derecho de información del interesado establecido en el artículo 21 cuando no se facilite toda la información exigida en esta Ley Orgánica.

c) La inobservancia de la obligación de informar al interesado y a los destinatarios a los que se hayan comunicado o de los que procedan los datos personales rectificadas, suprimidos o respecto de los que se haya limitado el tratamiento, conforme a lo establecido en el artículo 23.

d) El incumplimiento de la llevanza de registros de actividades de tratamiento o del registro de operaciones o que los mismos no incorporen toda la información exigida legalmente, siempre que no constituya infracción grave.

e) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando fuera exigible legalmente.

f) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas, a propósito del tratamiento de datos personales y de sus relaciones con los interesados, así como la inexactitud o la falta de concreción en la determinación de las mismas.

g) El incumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de una posible infracción de las disposiciones de esta Ley Orgánica, como consecuencia de una instrucción recibida de este.

h) La notificación incompleta o defectuosa a la autoridad de protección de datos competente de la información relacionada con una violación de seguridad de los datos personales, el incumplimiento de la obligación de documentarla o del deber de comunicar al interesado su existencia, cuando no constituya una infracción grave.

i) La aportación de información inexacta o incompleta a la autoridad de protección de datos competente, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa.

j) La falta de publicación de los datos de contacto del delegado de protección de datos, o la ausencia de comunicación de su designación y cese a la autoridad de protección de datos competente, de conformidad con el artículo 40, cuando su nombramiento sea exigible de acuerdo con esta Ley Orgánica.

Artículo 61. *Régimen jurídico.*

1. El ejercicio de la potestad sancionadora que corresponde a las autoridades de protección de datos competentes, se regirá por lo dispuesto en el presente capítulo, por los títulos VII y IX de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en cuanto no la contradiga, con carácter supletorio, por la normativa sobre el procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público.

2. En el supuesto de las infracciones recogidas en los artículos 58. j) y 59. j), el ejercicio de la potestad sancionadora corresponderá respectivamente, a las personas titulares de la Secretaría de Estado de Seguridad y de las Delegaciones del Gobierno. Estos procedimientos se regirán por la normativa sobre procedimiento administrativo común de las Administraciones Públicas y el régimen jurídico del sector público, sin perjuicio de las especialidades que se recogen en este capítulo.

Artículo 62. *Sanciones.*

Por la comisión de las infracciones tipificadas en esta Ley Orgánica se impondrán las siguientes sanciones:

1. En caso de que el sujeto responsable sea algunos de los enumerados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, se impondrán las sanciones y se adoptarán las medidas establecidas en dicho artículo.

2. En caso de que el sujeto infractor sea distinto de los señalados en el artículo 77.1 de la Ley Orgánica 3/2018, de 5 de diciembre, podrá ser sancionado, con multa de la siguiente cuantía:

- a) Las infracciones muy graves, con multa de 360.001 a 1.000.000 euros.
- b) Las infracciones graves, con multa de 60.001 a 360.000 euros.
- c) Las leves, con multa de 6.000 a 60.000 euros.

A efectos de la determinación de la cuantía de la sanción, se tendrán en cuenta los criterios establecidos en el artículo 83.2 del Reglamento General de Protección de Datos y en el artículo 76.2 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 63. *Prescripción de las infracciones y sanciones.*

1. Las infracciones administrativas tipificadas en esta Ley Orgánica prescribirán a los seis meses, a los dos o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.

Los plazos señalados en esta Ley Orgánica se computarán desde el día en que se haya cometido la infracción. No obstante, en los casos de infracciones continuadas o permanentes, los plazos se computarán desde que finalizó la conducta infractora.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Se interrumpirá igualmente la prescripción como consecuencia de la apertura de un procedimiento judicial penal, hasta que la autoridad judicial comunique al órgano administrativo su finalización.

2. Las sanciones impuestas por infracciones muy graves prescribirán a los tres años, las impuestas por infracciones graves, a los dos años, y las impuestas por infracciones leves al año, computados desde el día siguiente a aquel en que adquiera firmeza en vía administrativa la resolución por la que se impone la sanción.

La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 64. *Caducidad del procedimiento.*

1. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concorra identidad de sujeto, hecho y fundamento, hasta la finalización de este.

2. La resolución que declare la caducidad se notificará al interesado y pondrá fin al procedimiento, sin perjuicio de que la administración pueda acordar la incoación de un nuevo procedimiento en tanto no haya prescrito la infracción. Los procedimientos caducados no interrumpirán el plazo de prescripción.

Artículo 65. *Carácter subsidiario del procedimiento administrativo sancionador respecto del penal.*

1. No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente cuando se aprecie identidad de sujeto, de hecho y de fundamento.

2. En los supuestos en que las conductas pudieran ser constitutivas de delito, el órgano administrativo pasará el tanto de culpa a la autoridad judicial o al Ministerio Fiscal y se abstendrá de seguir el procedimiento sancionador mientras la autoridad judicial no dicte sentencia firme o resolución que de otro modo ponga fin al procedimiento penal, o el Ministerio Fiscal no acuerde la improcedencia de iniciar o proseguir las actuaciones en vía penal, quedando hasta entonces interrumpido el plazo de prescripción.

La autoridad judicial y el Ministerio Fiscal comunicarán al órgano administrativo la resolución o acuerdo que hubieran adoptado.

3. De no haberse estimado la existencia de ilícito penal, o en el caso de haberse dictado resolución de otro tipo que ponga fin al procedimiento penal, podrá iniciarse o proseguir el procedimiento sancionador. En todo caso, el órgano administrativo quedará vinculado por los hechos declarados probados en vía judicial.

4. Las medidas cautelares adoptadas antes de la intervención judicial podrán mantenerse mientras la autoridad judicial no resuelva otra cosa.

Disposición adicional primera. *Regímenes específicos.*

1. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, para los fines previstos en el artículo 1, se regirá por esta Ley Orgánica, sin perjuicio de los requisitos establecidos en regímenes legales especiales que regulan otros ámbitos concretos como el procesal penal, la regulación del tráfico o la protección de instalaciones propias.

2. Fuera de estos supuestos, dichos tratamientos se regirán por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y por la Ley Orgánica 3/2018, de 5 de diciembre.

Disposición adicional segunda. *Intercambio de datos dentro de la Unión Europea.*

El intercambio de datos personales por parte de las autoridades competentes españolas en el interior de la Unión Europea, cuando el Derecho de la Unión Europea o la legislación española exijan dicho intercambio, no estará limitado ni prohibido por motivos relacionados con la protección de las personas físicas respecto al tratamiento de sus datos personales.

Disposición adicional tercera. *Acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial.*

Los acuerdos internacionales en el ámbito de la cooperación judicial en materia penal y de la cooperación policial que impliquen la transferencia de datos personales a Estados que no sean miembros de la Unión Europea u organizaciones internacionales y que hubieran sido celebrados por España antes del 6 de mayo de 2016, cumpliendo lo dispuesto en el

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

Derecho de la Unión Europea aplicable antes de dicha fecha, seguirán en vigor hasta que sean objeto de modificación, enmienda o terminación.

Disposición adicional cuarta. *Ficheros y Registro de Población de las Administraciones Públicas.*

1. Las autoridades competentes podrán solicitar al Instituto Nacional de Estadística y a los órganos estadísticos de ámbito autonómico, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del documento de identidad, nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en el padrón municipal de habitantes y en el censo electoral correspondiente a los territorios donde ejerzan sus competencias. Esta solicitud deberá estar motivada en base a cualquiera de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.

2. Los datos obtenidos tendrán como único propósito el cumplimiento de los fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, así como de protección y de prevención frente a las amenazas contra la seguridad pública y la comunicación de estas autoridades con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico-administrativas derivadas de las competencias respectivas.

Disposición adicional quinta. *Referencias normativas.*

Las referencias contenidas en normas vigentes en relación a las disposiciones que se derogan expresamente, deberán entenderse efectuadas a los artículos de esta Ley Orgánica que regulan la misma materia que aquellas.

Disposición transitoria única. *Duración del mandato inicial de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial.*

La duración del mandato del primer nombramiento de la persona titular de la Dirección de Supervisión y Control de Protección de datos del Consejo General del Poder Judicial será de tres años no renovable.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en esta Ley Orgánica.

Disposición final primera. *Modificación de la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria.*

Se introduce un nuevo artículo 15 bis en la Ley Orgánica 1/1979, de 26 de septiembre, General Penitenciaria, que queda redactado como sigue:

«Artículo 15 bis. *Tratamientos de datos de carácter personal.*

1. Admitido en el establecimiento un interno, se procederá a verificar su identidad personal, efectuando la reseña alfabética, dactilar y fotográfica, así como a la inscripción en el libro de ingresos y a la apertura de un expediente personal relativo a su situación procesal y penitenciaria, respecto del que se reconoce el derecho de acceso. Este derecho sólo se verá limitado de forma individualizada y fundamentada en concretas razones de seguridad o tratamiento.

2. El tratamiento de los datos personales de los internos se regirá por lo previsto en la Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Los datos personales de categorías especiales que no figuren en el apartado anterior se podrán tratar con el consentimiento del interesado. Sólo se prescindirá de dicho consentimiento cuando sea estrictamente necesario y se efectúe con las garantías adecuadas para proteger el derecho a la

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

protección de datos de los interesados, atendiendo al tipo de datos que se traten y a las finalidades de los distintos tratamientos dirigidos a la ejecución de la pena.

3. Igualmente se procederá al cacheo de su persona y al registro de sus efectos, retirándose los enseres y objetos no autorizados.

4. En el momento del ingreso se adoptarán las medidas de higiene personal necesarias, entregándose al interno las prendas de vestir adecuadas que precise, firmando el mismo su recepción.»

Disposición final segunda. *Modificación de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal.*

Uno. Se modifica el artículo 12 para incluir en nuevo apartado n) con la siguiente redacción:

«n) La Unidad de Supervisión y Control de Protección de Datos.»

Dos. Se modifica el artículo 20 incluyendo un nuevo apartado Cuatro con la siguiente redacción:

«Cuatro. En la Fiscalía General del Estado, de igual modo, existirá la Unidad de Supervisión y Control de Protección de Datos que ejercerá las competencias que corresponden a la autoridad de protección de datos con fines jurisdiccionales sobre el tratamiento de los mismos realizado por el Ministerio Fiscal, de acuerdo con lo establecido en el artículo 236 octies de la Ley Orgánica del Poder Judicial en el ámbito de sus competencias y facultades. Su regulación se remitirá a los términos previstos en la Ley Orgánica del Poder Judicial en cuanto le sea de aplicación.

Al frente de la Unidad de Supervisión y Control de Protección de Datos se nombrará por mayoría absoluta del Pleno del Consejo Fiscal una persona titular de la Unidad, de entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

La duración del mandato de la persona titular de la Unidad de Supervisión y Control de Protección de Datos será de cinco años, no renovable. Durante su mandato permanecerá, en su caso, en situación de servicios especiales y ejercerá exclusivamente las funciones inherentes a su cargo. Sólo podrá ser cesada por incapacidad o incumplimiento grave de sus deberes, apreciados por el Pleno mediante mayoría absoluta.

El régimen de incompatibilidades de la persona titular de la Unidad de Supervisión y Control de Protección de Datos será el mismo que el establecido para los Fiscales al servicio de los órganos técnicos de la Fiscalía General del Estado. La persona titular de la Unidad de Supervisión y Control de Protección de Datos deberá ejercer sus funciones con absoluta independencia y neutralidad.

La persona titular y el resto de personal adscrito a la Unidad de Supervisión y Control de Protección de Datos estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Unidad de Supervisión y Control de Protección de Datos en materia de infracciones de la presente normativa.

La composición, organización y funcionamiento de la Unidad de Supervisión y Control de Protección de Datos será regulada reglamentariamente. Se deberá velar porque la Unidad cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.»

Tres. Se modifica el artículo 14 para incluir en el apartado 4 una nueva letra l) con el contenido siguiente:

«l) Nombrar por mayoría absoluta a la persona titular de la Unidad de Supervisión y Control de Protección de Datos.»

Disposición final tercera. *Modificación de la Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial.*

Los artículos que se relacionan quedarán modificados en los términos siguientes:

Uno. El artículo 234 queda redactado como sigue:

«Artículo 234.

1. Los Letrados de la Administración de Justicia y funcionarios competentes de la oficina judicial y de la oficina fiscal facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones procesales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas o reservadas conforme a la ley.

2. Las partes y cualquier persona que acredite un interés legítimo y directo tendrán derecho a obtener, en la forma dispuesta en las leyes procesales y, en su caso, en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados. También tendrán derecho a que se les expidan los testimonios y certificados en los casos y a través del cauce establecido en las leyes procesales.»

Dos. El artículo 235 queda redactado como sigue:

«Artículo 235.

El acceso a las resoluciones judiciales, o a determinados extremos de las mismas, o a otras actuaciones procesales, por quienes no son parte en el procedimiento y acrediten un interés legítimo y directo, podrá llevarse a cabo previa disociación, anonimización u otra medida de protección de los datos de carácter personal que las mismos contuvieren y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.»

Tres. El artículo 235 bis queda redactado como sigue:

«Artículo 235 bis.

1. Es público el acceso a los datos personales contenidos en los fallos de las sentencias firmes condenatorias, cuando se hubieren dictado en virtud de los delitos previstos en los siguientes artículos:

- a) Los artículos 305, 305 bis y 306 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- b) Los artículos 257 y 258 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, cuando el acreedor defraudado hubiese sido la Hacienda Pública.
- c) El artículo 2 de la Ley Orgánica 12/1995, de 12 de diciembre, de Represión del Contrabando, siempre que exista un perjuicio para la Hacienda Pública estatal o de la Unión Europea.

2. En los casos previstos en el apartado anterior, el Letrado de la Administración de Justicia emitirá certificado en el que se harán constar los siguientes datos:

- a) Los que permitan la identificación del proceso judicial.
- b) Nombre y apellidos o denominación social del condenado y, en su caso, del responsable civil.
- c) Delito por el que se le hubiera condenado.
- d) Las penas impuestas.
- e) La cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, según lo establecido en la sentencia.

Mediante diligencia de ordenación el Letrado de la Administración de Justicia ordenará su publicación en el «Boletín Oficial del Estado».

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

3. Lo dispuesto en este artículo no será de aplicación en el caso de que el condenado o, en su caso, el responsable civil, hubiera satisfecho o consignado en la cuenta de depósitos y consignaciones del órgano judicial competente la totalidad de la cuantía correspondiente al perjuicio causado a la Hacienda Pública por todos los conceptos, con anterioridad a la firmeza de la sentencia.»

Cuatro. El artículo 236 queda redactado como sigue:

«Artículo 236.

La publicidad de los edictos se realizará a través del Tablón Edictal Judicial Único, en la forma en que se disponga reglamentariamente, incluyendo los datos estrictamente necesarios para cumplir con su finalidad.»

Cinco. El artículo 236 bis queda redactado como sigue:

«Artículo 236 bis.

1. El tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional.

2. El tratamiento de los datos personales en la Administración de Justicia se llevará cabo por el órgano competente y, dentro de él, por quien tenga la competencia atribuida por la normativa vigente.»

Seis. El artículo 236 ter queda redactado como sigue:

«Artículo 236 ter.

1. El tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales.

2. En el ámbito de la jurisdicción penal, el tratamiento de los datos personales llevado a cabo con ocasión de la tramitación por los órganos judiciales y fiscalías de los procesos, diligencias o expedientes de los que sean competentes, así como el realizado dentro de la gestión de la Oficina judicial y fiscal, se regirá por lo dispuesto en la Ley Orgánica de protección de datos personales tratados con fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, sin perjuicio de las especialidades establecidas en el presente Capítulo y en las leyes procesales y, en su caso, en la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal.

3. No será necesario el consentimiento del interesado para que se proceda al tratamiento de los datos personales en el ejercicio de la actividad jurisdiccional, ya sean éstos facilitados por las partes o recabados a solicitud de los órganos competentes, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.»

Siete. El artículo 236 quáter queda redactado como sigue:

«Artículo 236 quáter.

Cuando se proceda al tratamiento con fines no jurisdiccionales se estará a lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y su normativa de desarrollo.»

Ocho. El artículo 236 quinquies queda redactado como sigue:

«Artículo 236 quinquies.

1. Las resoluciones y actuaciones procesales deberán contener los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, en especial para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

2. Los Jueces y Magistrados, los Fiscales y los Letrados de la Administración de Justicia, conforme a sus competencias, podrán adoptar las medidas que sean necesarias para la supresión de los datos personales de las resoluciones y de los documentos a los que puedan acceder las partes durante la tramitación del proceso siempre que no sean necesarios para garantizar el derecho a la tutela judicial efectiva, sin que, en ningún caso, pueda producirse indefensión.

3. Los datos personales que las partes conocen a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación también incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

4. Se deberán comunicar a los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de Justicia, en lo que proceda, los datos tratados con fines jurisdiccionales que sean estrictamente necesarios para el ejercicio de las funciones de inspección y control establecidas en esta Ley, y su normativa de desarrollo. También se deberán facilitar los datos tratados con fines no jurisdiccionales cuando ello esté justificado por la interposición de un recurso o sea necesario para el ejercicio de las competencias que tengan legalmente atribuidas.

5. Las Oficinas de Comunicación establecidas en esta Ley, en el ejercicio de sus funciones de comunicación institucional, deberán velar por el respeto del derecho fundamental a la protección de datos personales de aquellos que hubieran intervenido en el procedimiento de que se trate. Para cumplir con su finalidad, podrán recabar los datos necesarios de las autoridades competentes.

6. Los Letrados de la Administración de Justicia deberán facilitar a la Abogacía del Estado los datos personales, la información y los documentos que sean requeridos para el desempeño de la representación y defensa del Reino de España ante el Tribunal Europeo de Derechos Humanos y otros órganos internacionales en materia de protección de derechos Humanos, en particular ante el Comité de Naciones Unidas. A tales efectos, se establecerán igualmente los mecanismos de comunicación con la Fiscalía General del Estado, a través de sus unidades competentes.»

Nueve. El artículo 236 sexies queda redactado como sigue:

«Artículo 236 sexies.

1. La Administración competente deberá suministrar los medios tecnológicos adecuados para que se proceda al tratamiento de los datos personales conforme a las disposiciones legales y reglamentarias.

2. La Administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional.

3. Se deberán adoptar las medidas organizativas adecuadas para que la Oficina judicial y fiscal realice un adecuado tratamiento de los datos personales. Previo informe del Consejo General del Poder judicial, y, en su caso, de la Fiscalía General del Estado, el Ministerio de Justicia deberá elaborar y actualizar los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal, adecuando los principios de la normativa general a los propios de la regulación procesal y organización de la Oficina judicial y fiscal.

4. El Ministerio de Justicia y las Comunidades Autónomas con competencias en la materia, dentro de las políticas de apoyo a la Administración de Justicia y desarrollo de la gestión electrónica de los procedimientos, podrán realizar el

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

tratamiento de datos no personales para el ejercicio de sus competencias de gestión pública, incluyendo el desarrollo e implementación de sistemas automáticos de clasificación documental orientados a la tramitación procesal, con cumplimiento de la normativa de interoperabilidad, seguridad y protección de datos que resulte aplicable.»

Diez. El artículo 236 septies queda redactado como sigue:

«Artículo 236 septies.

1. En relación con el tratamiento de los datos personales con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación al proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante los órganos judiciales, fiscalías u Oficina judicial en los que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

2. En todo caso se denegará el acceso a los datos objeto de tratamiento con fines jurisdiccionales cuando las diligencias procesales en que se haya recabado la información sean o hayan sido declaradas secretas o reservadas.

3. En relación con el tratamiento de los datos personales con fines no jurisdiccionales, los interesados podrán ejercitar los derechos de información, acceso, rectificación, supresión, oposición y limitación en los términos establecidos en la normativa general de protección de datos.»

Once. El artículo 236 octies queda redactado como sigue:

«Artículo 236 octies.

1. Respecto a las operaciones de tratamiento efectuadas con fines jurisdiccionales por los Juzgados, Tribunales, Fiscalías, y las Oficinas judicial y fiscal, corresponderán al Consejo General del Poder Judicial y a la Fiscalía General del Estado, en el ámbito de sus respectivas competencias, las siguientes funciones:

a) Supervisar el cumplimiento de la normativa de protección de datos personales mediante el ejercicio de la labor inspectora otorgada en la presente Ley y el Estatuto Orgánico del Ministerio Fiscal.

b) Promover la sensibilización de los profesionales de la Administración de Justicia y su comprensión de los riesgos, normas, garantías, derechos y obligaciones en relación con el tratamiento.

c) Emitir informe sobre los códigos de conducta destinados a contribuir a la correcta aplicación de la normativa de protección de datos personales en la Oficina judicial y fiscal.

d) Previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en materia de protección de datos.

e) Tramitar y responder las reclamaciones presentadas por un interesado o por asociaciones, organizaciones y entidades que tengan capacidad procesal o legitimación para defender intereses colectivos, en los términos que determinen las leyes de aplicación al proceso en que los datos fueron recabados. Se informará al reclamante sobre el curso y resultado de la reclamación en un plazo razonable, previa realización de la investigación oportuna si se considera necesario.

2. Los tratamientos de datos con fines no jurisdiccionales estarán sometidos a la competencia de la Agencia Española de Protección de Datos, que también supervisará el cumplimiento de aquellos tratamientos que no sean competencia de las autoridades indicadas en el apartado anterior.

3. El Consejo General del Poder Judicial, la Fiscalía General del Estado y la Agencia Española de Protección de Datos colaborarán en aras del adecuado ejercicio de las respectivas competencias que la presente Ley Orgánica les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

4. Cuando con ocasión de la realización de actuaciones de investigación relacionadas con la posible comisión de una infracción de la normativa de protección de datos, las autoridades competentes a las que se refieran los apartados anteriores apreciaran la existencia de indicios que supongan la competencia de otra autoridad, darán inmediatamente traslado a esta última a fin de que prosiga con la tramitación del procedimiento.»

Doce. El artículo 236 nonies, queda redactado como sigue:

«Artículo 236 nonies.

1. Las competencias que corresponden a la autoridad de protección de datos personales con fines jurisdiccionales serán ejercidas respecto del tratamiento de los mismos realizado por Juzgados y Tribunales de acuerdo con lo establecido en el artículo 236 octies, por la Dirección de Supervisión y Control de Protección de Datos del Consejo General del Poder Judicial.

2. Al frente de la Dirección de Supervisión y Control de Protección de Datos se nombrará por mayoría absoluta del Pleno del Consejo General del Poder Judicial una persona titular de la Dirección, de entre juristas de reconocida competencia con al menos quince años de ejercicio profesional y con conocimientos y experiencia acreditados en materia de protección de datos.

3. La duración del mandato de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será de cinco años, no renovable. Durante su mandato permanecerá, en su caso, en situación de servicios especiales y ejercerá exclusivamente las funciones inherentes a su cargo. Sólo podrá ser cesada por incapacidad o incumplimiento grave de sus deberes, apreciados por el Pleno mediante mayoría absoluta.

4. El régimen de incompatibilidades de la persona titular de la Dirección de Supervisión y Control de Protección de Datos será el mismo que el establecido para los Magistrados al servicio de los órganos técnicos del Consejo General del Poder Judicial. La persona titular de la Dirección de Supervisión y Control de Protección de Datos deberá ejercer sus funciones con absoluta independencia y neutralidad.

5. La persona titular y el resto de personal adscrito a la Dirección de Supervisión y Control de Protección de Datos estarán sujetos al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus atribuciones. Este deber de secreto profesional se aplicará en particular a la información que faciliten las personas físicas a la Dirección de Supervisión y Control de Protección de Datos en materia de infracciones de la presente normativa.

6. La composición, organización y funcionamiento de la Dirección de Supervisión y Control de Protección de Datos será regulada reglamentariamente. El Consejo General del Poder Judicial deberá velar porque la Dirección cuente, en todo caso, con todos los medios personales y materiales necesarios para el adecuado ejercicio de sus funciones.»

Trece. El artículo 236 decies, queda redactado como sigue:

«Artículo 236 decies.

1. Los tratamientos de datos llevados a cabo por el Consejo General del Poder judicial y la Fiscalía General del Estado en el ejercicio de sus competencias quedarán sometidos a lo dispuesto en la legislación vigente en materia de protección de datos personales. Dichos tratamientos no serán considerados en ningún caso realizados con fines jurisdiccionales.

2. Las operaciones de tratamiento de datos personales del Consejo General del Poder Judicial y de los órganos integrantes del mismo serán autorizados por acuerdo del Consejo General del Poder Judicial, a propuesta de la Secretaría General, que ostentará la condición de responsable del tratamiento respecto de los mismos.

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

3. Las operaciones de tratamiento de datos personales de la Fiscalía General del Estado serán autorizadas según determine el Estatuto Orgánico del Ministerio Fiscal y las Instrucciones que se dicten al respecto.»

Catorce. El ordinal 19.º del apartado 1 del artículo 560 queda redactado como sigue:

«Artículo 560.

1.º (...)

19.º En materia de protección de datos personales, ejercerá las funciones definidas en el artículo 236 octies.»

Disposición final cuarta. *Modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Uno. Se incluye un nuevo apartado 5 en el artículo 2 con la siguiente redacción:

«Artículo 2.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se registrarán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.»

Dos. Se modifica el apartado 3 del artículo 44, que queda redactado como sigue:

«Artículo 44.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.»

Tres. Se modifica la disposición adicional decimoquinta que queda redactada como sigue:

«Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.»

Disposición final quinta. *Modificación de la Ley Orgánica 1/2020, de 16 de septiembre, sobre la utilización de los datos del registro de nombres de pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.*

Se modifica el artículo 10 que queda redactado como sigue:

«1. Los momentos en los que las compañías aéreas deben transmitir los datos PNR a la UIP serán los siguientes:

a) Entre las 24 y las 48 horas antes de la hora de salida programada del vuelo, e

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

b) inmediatamente después del cierre del vuelo, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar o desembarcar.

Las compañías aéreas podrán limitar esta transmisión prevista en el párrafo b) a las actualizaciones de la información transmitida conforme al párrafo a).

2. El Proveedor de Servicios de Navegación Aérea en el espacio aéreo de soberanía española, comunicará a la UIP los cambios de destino, así como las escalas no programadas que le sean notificados por la tripulación de la aeronave o por otro Proveedor de Servicios de Navegación Aérea».

3. Además, cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta relacionada con delitos de terrorismo o con delitos graves, en momentos distintos de los previstos en el apartado 1, todos los sujetos obligados, caso por caso, deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.»

Disposición final sexta. *Modificación de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.*

Se modifica el artículo 30 que queda redactado como sigue:

«Artículo 30. *Procedimiento sancionador.*

1. El ejercicio de la potestad sancionadora a la que se refiere este título, se regirá por lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este título.

2. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concorra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.»

Disposición final séptima. *Modificación de la Ley 5/2014, de 4 de abril, de Seguridad Privada.*

Se modifica el artículo 69 que queda redactado como sigue:

«Artículo 69. *Régimen Jurídico.*

1. El ejercicio de la potestad sancionadora en materia de seguridad privada se regirá por lo dispuesto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y sus disposiciones de desarrollo, sin perjuicio de las especialidades que se regulan en este título.

2. El procedimiento caducará transcurridos seis meses desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concorra identidad de sujeto, hecho y fundamento, hasta la finalización de éste.

3. Iniciado el procedimiento sancionador, el órgano que haya ordenado su incoación podrá adoptar las medidas cautelares necesarias para garantizar su adecuada instrucción, así como para evitar la continuación de la infracción o asegurar el pago de la sanción, en el caso de que ésta fuese pecuniaria, y el cumplimiento de la misma en los demás supuestos.

4. Dichas medidas, que deberán ser congruentes con la naturaleza de la presunta infracción y proporcionadas a la gravedad de la misma, podrán consistir en:

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

a) La ocupación o precinto de vehículos, armas, material o equipo prohibido, no homologado o que resulte peligroso o perjudicial, así como de los instrumentos y efectos de la infracción.

b) La retirada preventiva de las autorizaciones, habilitaciones, permisos o licencias, o la suspensión, en su caso, de la eficacia de las declaraciones responsables.

c) La suspensión de la habilitación del personal de seguridad privada y, en su caso, de la tramitación del procedimiento para el otorgamiento de aquélla, mientras dure la instrucción de expedientes por infracciones graves o muy graves en materia de seguridad privada.

También podrán ser suspendidas las indicadas habilitación y tramitación, hasta tanto finalice el proceso por delitos contra dicho personal.

5. Las medidas cautelares previstas en los párrafos b) y c) del apartado anterior no podrán tener una duración superior a un año.»

Disposición final octava. *Modificación del texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por el Real Decreto Legislativo 6/2015, de 30 de octubre.*

Se modifica el artículo 68 que queda redactado como sigue:

«**Artículo 68.** *Matrículas.*

1. Para poner en circulación vehículos a motor, así como remolques de masa máxima autorizada superior a la que reglamentariamente se determine, es preciso matricularlos y que lleven las placas de matrícula con los caracteres que se les asigne del modo que se establezca. Esta obligación será exigida a los ciclomotores en los términos que reglamentariamente se determine.

2. Deben ser objeto de matriculación definitiva en España los vehículos a los que se refiere el apartado anterior, cuando se destinen a ser utilizados en el territorio español por personas o entidades que sean residentes en España o que sean titulares de establecimientos situados en España. Reglamentariamente se establecerán los plazos, requisitos y condiciones para el cumplimiento de esta obligación y las posibles exenciones a la misma.

3. La matriculación ordinaria será única para cada vehículo, salvo en los supuestos que se determinen reglamentariamente. Cuando concurren circunstancias que puedan afectar a la Seguridad Nacional, el Secretario de Estado de Seguridad podrá autorizar una nueva matrícula distinta de la inicialmente asignada. Este tipo de matrículas no serán públicas en el Registro General de Vehículos e, incluso en circunstancias excepcionales, podrá utilizarse una titularidad supuesta en el marco de la actuación de las Fuerzas y Cuerpos de Seguridad y del Centro Nacional de Inteligencia en el tráfico jurídico.

4. En casos justificados, la autoridad competente para expedir el permiso de circulación podrá conceder permisos de circulación temporales y provisionales en los términos que se determine reglamentariamente.»

Disposición final novena. *Naturaleza de la ley.*

Esta ley tiene el carácter de Ley Orgánica. No obstante, tienen carácter ordinario:

- a) El capítulo VI.
- b) El capítulo VII.
- c) El capítulo VIII.
- d) Las disposiciones finales segunda, sexta, séptima y octava.

Disposición final décima. *Título competencial.*

Esta Ley Orgánica se dicta al amparo de las reglas 1.^a, 6.^a, 18.^a y 29.^a del artículo 149.1 de la Constitución, que atribuyen al Estado las competencias exclusivas, respectivamente, para la regulación de las condiciones básicas que garanticen la igualdad de todos los

§ 3 Ley Orgánica de protección de datos para enjuiciamiento de infracciones penales

españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales; respecto a las bases del régimen jurídico de las Administraciones Públicas, el procedimiento administrativo común y en relación al sistema de responsabilidad de todas las Administraciones públicas; sobre legislación penal, penitenciaria, procesal; y en materia de seguridad pública.

Disposición final undécima. *Incorporación del Derecho de la Unión Europea.*

Mediante esta Ley Orgánica se incorpora al ordenamiento jurídico español la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Disposición final duodécima. *Entrada en vigor.*

Esta Ley Orgánica entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

No obstante, las previsiones contenidas en el capítulo IV producirán efectos a los seis meses de la entrada en vigor de la Ley Orgánica.

§ 4

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 218, de 8 de septiembre de 2018
Última modificación: 30 de marzo de 2022
Referencia: BOE-A-2018-12257

[...]

TÍTULO III

Marco estratégico e institucional

[...]

Artículo 10. *Funciones de las autoridades competentes.*

Las autoridades competentes ejercerán las siguientes funciones:

- a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.
- b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.
- c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.
- d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de este real decreto-ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.
- e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de este real decreto-ley, conforme a lo establecido en el artículo 27.
- f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 26.
- g) Cooperar, en el ámbito de aplicación de este real decreto-ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes, conforme a lo establecido en los artículos 14 y 29.
- h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 16 y 19.

§ 4 Real Decreto-ley de seguridad de las redes y sistemas de información [parcial]

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 17.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 25.

Artículo 11. *Equipos de respuesta a incidentes de seguridad informática de referencia.*

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

[...]

Artículo 14. *Cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales.*

1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.

2. Consultarán así mismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de este real decreto-ley, y colaborarán con ellos en el ejercicio de sus funciones.

3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello.

[...]

TÍTULO V

Notificación de incidentes

[...]

Artículo 29. *Cooperación en lo relativo a los incidentes que afecten a datos personales.*

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.

[...]

Disposición adicional tercera. *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley.*

La plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

[...]

§ 5

Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones

Jefatura del Estado
«BOE» núm. 266, de 5 de noviembre de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-15790

I

La sociedad actual requiere de adaptaciones en la esfera digital que exigen de una traducción en el plano normativo. El desarrollo y empleo de las nuevas tecnologías y redes de comunicaciones por parte de las Administraciones Públicas se está acelerando. Ello exige establecer sin demora un marco jurídico que garantice el interés general y, en particular, la seguridad pública, asegurando la adecuada prestación de los servicios públicos y, al mismo tiempo, que la administración digital se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos.

El carácter estratégico para la seguridad pública de las materias reguladas en este real decreto-ley se ve avalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que describe los riesgos asociados a las nuevas tecnologías como uno de los principales desafíos de la sociedad actual.

La Estrategia de Seguridad Nacional 2017, aprobada mediante Real Decreto 1008/2017, de 1 de diciembre, identifica las ciberamenazas y el espionaje como amenazas que comprometen o socavan la seguridad nacional y, en coherencia con ello, singulariza la ciberseguridad como uno de sus ámbitos prioritarios de actuación. El desarrollo tecnológico implica una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos e información, el *hackeo* de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas. La hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública y exige una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

Entre los principales desafíos que las nuevas tecnologías plantean desde el punto de vista de la seguridad pública se encuentran las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje. Estas actividades se benefician de las posibilidades que ofrece la sofisticación informática para acceder a ingentes volúmenes de información y datos sensibles.

En este punto juega un papel decisivo el proceso de transformación digital de la Administración, ya muy avanzado. La administración electrónica agudiza la dependencia de las tecnologías de la información y extiende la posible superficie de ataque, incrementando

el riesgo de utilización del ciberespacio para la realización de actividades ilícitas que impactan en la seguridad pública y en la propia privacidad de los ciudadanos.

Los recientes y graves acontecimientos acaecidos en parte del territorio español han puesto de relieve la necesidad de modificar el marco legislativo vigente para hacer frente a la situación. Tales hechos demandan una respuesta inmediata para evitar que se reproduzcan sucesos de esta índole estableciendo un marco preventivo a tal fin, cuyo objetivo último sea proteger los derechos y libertades constitucionalmente reconocidos y garantizar la seguridad pública de todos los ciudadanos.

El presente real decreto-ley tiene por objeto regular este marco normativo, que comprende medidas urgentes relativas a la documentación nacional de identidad; a la identificación electrónica ante las Administraciones Públicas; a los datos que obran en poder de las Administraciones Públicas; a la contratación pública y al sector de las telecomunicaciones.

II

El presente real decreto-ley consta de una parte expositiva y una parte dispositiva estructurada del modo siguiente: capítulo I (artículos 1 y 2), un capítulo II (artículos 3 y 4), un capítulo III (artículo 5), un capítulo IV (artículo 6), un capítulo V (artículo 7), una disposición adicional, tres disposiciones transitorias y tres disposiciones finales.

El capítulo I contempla dos medidas en materia de documentación nacional de identidad, dirigidas a configurar el Documento Nacional de Identidad, con carácter exclusivo y excluyente, como el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular. Con esta finalidad, el artículo 1 del presente real decreto-ley modifica el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. En coherencia con ello, el artículo 2 del real decreto-ley modifica la regulación del Documento Nacional de Identidad electrónico recogida en el artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El capítulo II del presente real decreto-ley, que contiene los artículos 3 y 4, establece varias medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas. La finalidad de estas medidas es garantizar la seguridad pública, tanto en las relaciones entre las distintas Administraciones Públicas cuando traten datos personales, como entre ciudadanos y Administraciones Públicas cuando las últimas proceden a la recopilación, tratamiento y almacenamiento de datos personales en ejercicio de una función pública.

El artículo 3 del presente real decreto-ley modifica los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a la vez que introduce una nueva disposición adicional sexta a la misma.

La modificación de la letra a) del apartado 2 de los artículos 9 y 10 responde a la necesidad de adaptar sus contenidos al Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, conocido como Reglamento eIDAS, que establece un marco legal común para las identificaciones y firmas electrónicas en la Unión Europea.

La modificación de la letra c) del apartado 2 de los artículos 9 y 10 tiene como finalidad garantizar la seguridad pública en relación con el empleo de sistemas de identificación y firma electrónicas de los interesados cuando se realizan con clave concertada o mediante cualquier otro sistema que cuente con un registro previo como usuario que permita garantizar su identidad y que las Administraciones Públicas consideren válido. Así, en palabras del propio Tribunal Constitucional expresadas en la Sentencia 55/2018, de 24 de mayo, se mantiene la posibilidad de que «cada administración diseñe sus propios sistemas de identificación electrónica o admita los expedidos por otras entidades públicas o privadas y, con ello, que estos sean más o menos complejos según sus preferencias y la relevancia o características del trámite o servicio correspondiente». Ahora bien, para garantizar la seguridad pública, competencia exclusiva del Estado conforme dispone el artículo 1.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, la modificación efectuada somete a un régimen de autorización previa por parte de la Administración

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

General del Estado a los sistemas que sean distintos a aquellos del certificado y sello electrónico. Dicha autorización tendrá por objeto, exclusivamente, verificar si el sistema validado tecnológicamente por parte de la Administración u Organismo Público de que se trate puede o no producir afecciones o riesgos a la seguridad pública, de modo que, si así fuera y solo en este caso, la Administración del Estado denegará dicha autorización con base en dichas consideraciones de seguridad pública.

En la misma línea, el nuevo apartado 3, que se añade tanto al artículo 9 como al artículo 10 de la Ley 39/2015, de 1 de octubre, establece la obligatoriedad de que, en relación con los sistemas previstos en la letra c) del apartado 2 de los artículos 9 y 10, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Salvo las excepciones que se introducen en la ley, estos datos no podrán ser objeto de transferencia a un tercer país u organización internacional y, en cualquier caso, se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Por último, el artículo 3 del presente real decreto-ley incorpora una disposición adicional sexta a la Ley 39/2015, de 1 de octubre, que prevé que en las relaciones de los interesados con las Administraciones Públicas no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Además, la nueva disposición adicional sexta establece que cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública. La falta de un marco regulatorio *ad hoc* sobre estas nuevas tecnologías justifica que, con carácter urgente y en ejercicio de su competencia para dictar legislación básica, el Estado intervenga sobre la materia con carácter provisional hasta que se avance en el seno de la Unión Europea en el tratamiento de este tipo de tecnologías.

El artículo 4 del presente real decreto-ley procede, por una parte, a la modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público introduciendo un nuevo artículo 46 bis, y dando una nueva redacción al artículo 155.

Por una parte, el artículo 46 bis obliga a que, por motivos de seguridad pública, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, se ubiquen y presten dentro del territorio de la Unión Europea. Asimismo, establece que solo puedan ser cedidos a terceros países cuando estos cumplan con las garantías suficientes que les permitan haber sido objeto de una decisión de adecuación de la Comisión Europea, o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

Por otra parte, la finalidad de la modificación del artículo 155 es permitir un mayor control de los datos cedidos entre Administraciones Públicas, al efecto de garantizar la adecuada utilización de los mismos. Se permite excepcionalmente que la Administración General del Estado pueda adoptar la medida de suspender la transmisión de datos por razones de

seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación.

La licitud del tratamiento de los datos personales para finalidades distintas de las finalidades iniciales viene determinada por la circunstancia de que se trate de finalidades compatibles. Tratándose de finalidades incompatibles, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, prohíbe su tratamiento. No obstante, el propio Reglamento declara ya unas finalidades que estima compatibles: tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. En este sentido, en caso de que el responsable del tratamiento (el cesionario), previo análisis de la compatibilidad de acuerdo con los criterios del artículo 6.4 del citado Reglamento, considere que es compatible, el precepto introduce la obligación adicional de consultar a la administración cedente. La Administración General del Estado podrá oponerse motivadamente y suspender por razones de seguridad nacional.

El capítulo III del presente real decreto-ley regula varias medidas en materia de contratación pública, todas ellas dirigidas a reforzar el cumplimiento de la normativa sobre protección de datos personales y la protección de la seguridad pública en este ámbito.

Los contratistas del sector público manejan en ocasiones, para la ejecución de los respectivos contratos, un ingente volumen de datos personales, cuyo uso inadecuado puede, a su vez, plantear riesgos para la seguridad pública. Por ello, resulta necesario asegurar normativamente su sometimiento a ciertas obligaciones específicas que garanticen tanto el cumplimiento de la normativa en materia de protección de datos personales como la protección de la seguridad pública.

El real decreto-ley modifica la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, con la finalidad de introducir medidas que garanticen en todas las fases de la contratación (expediente de contratación, licitación y ejecución del contrato) el respeto por parte de contratistas y subcontratistas de la legislación de la Unión Europea en materia de protección de datos.

Dichas modificaciones son coherentes con lo previsto en el artículo 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que, respecto de los tratamientos de datos necesarios para el cumplimiento de una obligación legal o de una misión realizada en interés público o en el ejercicio de poderes públicos, permite a los Estados miembros que mantengan o introduzcan disposiciones específicas para fijar los requisitos específicos del tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo.

Así, en primer lugar, el presente real decreto-ley modifica el artículo 35 de la Ley 9/2017, de 8 de noviembre, para incluir, como contenido mínimo de los contratos, la referencia expresa al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

En segundo lugar, y por lo que respecta al régimen de invalidez de los contratos, se añade un subapartado al artículo 39.2 de la Ley 9/2017, de 8 de noviembre, para incluir, como causa de nulidad de pleno derecho, la celebración de contratos por parte de poderes adjudicadores que omitan mencionar en los pliegos las obligaciones del futuro contratista en materia de protección de datos a los que se refiere el nuevo artículo 122.2 de la Ley 9/2017, en la redacción dada a dicho precepto por el presente real decreto-ley. La aplicación en este caso de la consecuencia jurídica máxima que contempla nuestro ordenamiento jurídico, esto es, de la nulidad de pleno Derecho, se ha considerado adecuada una vez ponderada la oportunidad de su incorporación en la legislación de contratos del sector público (siguiéndose el dictamen n. 116/2015, del Consejo de Estado), dada la importancia que en determinados casos puede presentar para los intereses de la seguridad nacional conocer la ubicación de los servidores en los que se alojarán los datos que ceda la Administración con motivo de la ejecución de un contrato público, desde dónde se van a prestar los servicios asociados a los mismos y asegurar el sometimiento de la ejecución de ese contrato a la normativa nacional y de la Unión Europea en materia de protección de datos.

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

En tercer lugar, y en el contexto de la regulación de los requisitos para contratar con el sector público, se modifica el artículo 116.1 de la Ley 9/2017, de 8 de noviembre, para incluir, como circunstancia que impedirá a los empresarios contratar con las entidades comprendidas en el artículo 3 de dicha Ley, el haber dado lugar a la resolución firme de cualquier contrato celebrado con una de tales entidades por incumplimiento culpable de las obligaciones que los pliegos hubieren calificado como esenciales de acuerdo con lo previsto en el art. 211.1.f) de la propia Ley.

En cuarto lugar, se da una nueva redacción al artículo 116.1 de la Ley 9/2017, de 8 de noviembre, introduciendo un segundo párrafo relativo al expediente de contratación de los contratos cuya ejecución requiera de la cesión de datos por parte de entidades del sector público al contratista. En virtud de esta modificación, se incluye la obligación del órgano de contratación de especificar en el expediente cuál será la finalidad de los datos que vayan a ser cedidos.

En quinto lugar, se da una nueva redacción al artículo 122.2 de la Ley 9/2017, de 8 de noviembre, relativo a los pliegos de cláusulas administrativas particulares. En concreto, se añade un párrafo tercero a este apartado para incluir la obligación de los pliegos de mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos. Asimismo, se añade un párrafo cuarto relativo a los contratos que exijan el tratamiento por el contratista de datos personales por parte del responsable del tratamiento, indicando que en estos casos será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener al contratante al corriente de la ubicación de los correspondientes servidores. También se añade un párrafo quinto para establecer que los extremos mencionados en el párrafo cuarto deben hacerse constar en los pliegos como obligaciones esenciales a los efectos del régimen de resolución del contrato.

En sexto lugar, el presente real decreto-ley da una nueva redacción al artículo 202.1 de la Ley 9/2017, de 8 de noviembre, regulador de las condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental o de otro orden. En concreto, se introduce un párrafo tercero relativo a los pliegos correspondientes a contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista. Mediante esta adición se impone la exigencia de que los pliegos incluyan, como condición especial de ejecución, la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos. Asimismo, en los pliegos debe advertirse al contratista de que esta obligación tiene el carácter de obligación contractual esencial a los efectos del régimen de resolución del contrato.

En séptimo lugar, el artículo 5 siete del real decreto-ley da una nueva redacción al artículo 215.4 de la Ley 9/2017, relativo a la subcontratación, para incluir, entre las obligaciones del contratista principal, la de asumir la total responsabilidad de la ejecución del contrato frente a la Administración también por lo que respecta a la obligación de sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

El capítulo IV de este real decreto-ley regula varias medidas para reforzar la seguridad en materia de telecomunicaciones. Así, el artículo 6 de esta norma acomete cinco modificaciones de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, con el objetivo de potenciar las facultades de que dispone el Gobierno, a través del Ministerio de Economía y Empresa, para afrontar situaciones que pueden afectar al mantenimiento del orden público, la seguridad pública o la seguridad nacional.

Así, en concreto, se modifican los artículos 4.6 y 6.3 de la Ley 9/2014, de 9 de mayo, para reforzar las potestades del Ministerio de Economía y Empresa para llevar a cabo un mayor control y para mejorar sus posibilidades de actuación cuando la comisión de una presunta actuación infractora a través del uso de las redes y servicios de comunicaciones electrónicas pueda suponer una amenaza grave e inmediata para el orden público, la seguridad pública o la seguridad nacional o cuando en determinados supuestos excepcionales que también puedan comprometer el orden público, la seguridad pública y la seguridad nacional sea necesaria la asunción de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas.

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

Estas mayores posibilidades de actuación que se reconocen no se limitan en su aplicación a un concepto estricto de una red o un servicio de comunicaciones electrónicas, sino que extienden su eficacia a los elementos que necesariamente acompañan a la instalación o despliegue de una red o la prestación de un servicio de comunicaciones electrónicas, como son las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas, sus recursos asociados o cualquier elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

En necesaria correlación con este reforzamiento de funciones públicas en estas situaciones excepcionales, se potencia igualmente la potestad sancionadora del Ministerio de Economía y Empresa con el objetivo de hacer efectivas y reales las actuaciones que pueda adoptar en uso de estas nuevas facultades de actuación dirigidas a preservar o restablecer el orden público, la seguridad pública y la seguridad nacional. Con esta finalidad, el presente real decreto-ley da una nueva redacción a los artículos 76.15, 77.28 y 81.1 de la Ley 9/2014, de 9 de mayo. En particular, se amplían los supuestos en los que el Ministerio de Economía y Empresa puede adoptar medidas cautelares en casos de razones de imperiosa urgencia sin audiencia previa del presunto infractor, que puede incluir el cese de la actividad o la prestación de servicios, incorporando al efecto algunos de los supuestos que contemplados con dicha finalidad figuran en el artículo 30.6 del Código Europeo de las Comunicaciones Electrónicas, aprobado por la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, en especial, los relativos a la existencia de una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

Por último, el capítulo V incorpora medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información. Para ello, efectúa una modificación del real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en virtud de la cual el Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público. Adicionalmente, se prevé que el CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad.

III

El real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (Sentencias 6/1983, de 4 de febrero, F. 5; 11/2002, de 17 de enero, F. 4, 137/2003, de 3 de julio, F. 3 y 189/2005, de 7 julio, F.3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever exige una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las leyes.

En relación con la concurrencia de los presupuestos habilitantes de extraordinaria y urgente necesidad, debe tenerse en cuenta la doctrina de nuestro Tribunal Constitucional, resumida en el Fundamento Jurídico IV de la Sentencia 61/2018, de 7 de junio de 2018. De acuerdo con ella, se requieren, por un lado, «la presentación explícita y razonada de los motivos que han sido tenidos en cuenta por el Gobierno en su aprobación», es decir, lo que ha venido en denominarse, la situación de urgencia; y, por otro, «la existencia de una necesaria conexión entre la situación de urgencia definida y la medida concreta adoptada para subvenir a ella».

En cuanto a la situación de urgencia, el Tribunal Constitucional ha indicado que «aun habiendo descartado que la utilización por el Gobierno de su potestad legislativa extraordinaria deba circunscribirse a situaciones de fuerza mayor o emergencia, es lo cierto que hemos exigido la concurrencia de ciertas notas de excepcionalidad, gravedad, relevancia e imprevisibilidad que determinen la necesidad de una acción normativa inmediata en un plazo más breve que el requerido para la tramitación parlamentaria de las leyes, bien sea por el procedimiento ordinario o por el de urgencia» (SSTC 68/2007, FJ 10, y

137/2011, FJ 7). También ha señalado el Tribunal Constitucional que la valoración de la extraordinaria y urgente necesidad de una medida puede ser independiente de su imprevisibilidad e, incluso, de que tenga su origen en la previa inactividad del propio Gobierno, siempre que concurra efectivamente la excepcionalidad de la situación, pues «lo que aquí debe importar no es tanto la causa de las circunstancias que justifican la legislación de urgencia cuanto el hecho de que tales circunstancias efectivamente concurren» (STC 11/2002, de 17 de enero, FJ 6).

En cuanto a la conexión de sentido entre la situación de necesidad definida y las medidas que en el real decreto-ley se adoptan, el Tribunal Constitucional atiende a «un doble criterio o perspectiva para valorar la existencia de la conexión de sentido: el contenido, por un lado, y la estructura, por otro, de las disposiciones incluidas en el Real Decreto-ley controvertido» (SSTC 29/1982, de 31 de mayo, FJ 3; 1/2012, de 13 de enero, FJ 11; 39/2013, de 14 de febrero, FJ 9; y 61/2018, de 7 de junio, FJ 4).

La alternativa de introducir estas medidas mediante un proyecto de ley no es factible en el presente caso, habida cuenta de que las Cámaras se encuentran disueltas y no es posible dilatar su adopción hasta la constitución de las Cortes Generales, y, aun utilizándose entonces el trámite de urgencia, no se lograría reaccionar a tiempo.

Los motivos que acaban de exponerse justifican ampliamente la concurrencia de los requisitos constitucionales de extraordinaria y urgente necesidad, que habilitan al Gobierno para aprobar el presente real decreto-ley dentro del margen de apreciación que, en cuanto órgano de dirección política del Estado, le reconoce el artículo 86.1 de la Constitución (STC 142/2014, FJ 3 y STC 61/2018, FFJJ 4 y 7). Concurren también las notas de excepcionalidad, gravedad y relevancia que hacen necesaria una acción normativa inmediata en un plazo más breve que el requerido para la tramitación parlamentaria de una ley, bien sea por el procedimiento ordinario o por el de urgencia (STC 68/2007, FJ 10 y STC 137/2011, FJ 7).

Por lo demás, en el supuesto abordado por este real decreto-ley ha de subrayarse que para subvenir a la situación de extraordinaria y urgente necesidad descrita es necesario proceder a la reforma de varias normas con rango de ley, lo que de por sí exige «una respuesta normativa con rango de ley» (STC 152/2017, de 21 de diciembre, FJ 3 i).

IV

El presente real decreto-ley respeta los límites constitucionalmente establecidos para el uso de este instrumento normativo, pues no afecta al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el Título I de la Constitución, al régimen de las comunidades autónomas ni al Derecho electoral general.

Ciertamente, el presente real decreto-ley contiene varias medidas de modificación de leyes preexistentes que refuerzan el cumplimiento de la normativa en materia de protección de datos. No obstante, tales normas no constituyen una regulación del régimen general del derecho a la protección de datos, ni van en contra del contenido o elementos esenciales del este derecho, que son los contenidos prohibidos al instrumento jurídico del real decreto-ley según reiterada doctrina constitucional (sintetizada, recientemente, en la STC 139/2016, de 21 julio). Así, el presente real decreto-ley se limita a regular varios aspectos meramente puntuales respecto del tratamiento de datos personales por parte de las Administraciones Públicas y sus contratistas al amparo de la habilitación contenida en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por lo demás, este real decreto-ley no invade la reserva de ley orgánica prevista en el artículo 81 de la Constitución ni en ningún otro precepto constitucional, en tanto que no se modifican preceptos de carácter orgánico. En particular, carece de carácter orgánico el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, como expresamente dispone la Disposición Final Tercera de dicho texto legal.

V

El artículo 21.3 de la Ley 50/1997, de 27 de noviembre, del Gobierno, habilita al Gobierno en funciones para adoptar medidas distintas al despacho ordinario de los asuntos públicos en «casos de urgencia debidamente acreditados», así como «por razones de interés general cuya acreditación expresa así lo justifique».

Por su parte, los apartados 4 y 5 del artículo 21 de la Ley 50/1997, de 27 de noviembre, recogen una serie de facultades cuyo ejercicio está expresamente vedado al Gobierno en funciones, sin que ninguna de ellas se refiera a la aprobación de reales decretos-leyes. Dichas funciones de ejercicio prohibido para el Ejecutivo en funciones se refieren a cuestiones netamente distintas. En efecto, el artículo 21.4 establece que el Presidente del Gobierno en funciones no podrá proponer al Rey la disolución de alguna de las Cámaras, o de las Cortes Generales, ni plantear la cuestión de confianza, ni tampoco proponer al Rey la convocatoria de un referéndum consultivo. Por su parte, el artículo 21.5 de la Ley 50/1997, de 27 de noviembre, dispone que el Gobierno en funciones no podrá aprobar el Proyecto de Ley de Presupuestos Generales del Estado, ni tampoco presentar proyectos de ley al Congreso de los Diputados o, en su caso, al Senado.

La facultad del Gobierno en funciones de aprobar reales decretos leyes es congruente, por lo demás, con la exigencia de que concurra el presupuesto habilitante de extraordinaria y urgente necesidad previsto en el artículo 86 de la Constitución Española.

VI

El presente real decreto-ley se dicta al amparo de las competencias estatales contempladas en los apartados 18.^a, 21.^a y 29.^a del artículo 149.1 de la Constitución Española.

Por lo que respecta al artículo 149.1.18.^a de la Constitución Española, mediante el presente real decreto-ley se reforman las Leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, aprobadas por el legislador estatal en ejercicio de su competencia sobre las bases del régimen jurídico de las Administraciones Públicas y sobre el procedimiento administrativo común. Asimismo, el presente real decreto-ley procede a la modificación de varios preceptos de la Ley 9/2017, de 8 de noviembre, preceptos que se enmarcan en la competencia estatal sobre legislación básica en materia de contratos y concesiones administrativas.

En virtud del artículo 149.1.21.^a de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de correos y telecomunicaciones, el presente real decreto-ley modifica varios preceptos de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

En cuanto a las competencias exclusivas del Estado en materia de seguridad pública (artículo 149.1.29.^a de la Constitución Española), el presente real decreto-ley modifica la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y el mencionado Real Decreto-ley 12/2018. De acuerdo con este mismo título competencial, se modifica también la Ley 59/2003, de 19 de diciembre, de firma electrónica. Por último, es esta habilitación competencial la que ampara las modificaciones referidas a la necesaria autorización previa por parte de la Administración General del Estado de los sistemas de identificación y firma que cuenten con un registro previo como usuario.

Como se ha justificado en los apartados anteriores, las medidas contenidas en el presente real decreto-ley tienen como finalidad incrementar el estándar de protección de la seguridad pública frente a las crecientes amenazas que plantea el uso de las nuevas tecnologías y a la luz siempre de los últimos sucesos en territorio español. Ha de recordarse que, según la jurisprudencia constitucional, la seguridad pública se refiere a la «actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadanos»; aunque no se limita a regular «las actuaciones específicas de la llamada Policía de seguridad», pues «la actividad policial es una parte de la materia más amplia de la seguridad pública» que «abarca un amplio espectro de actuaciones administrativas» (STC 86/2014, de 29 de mayo, FFJJ 2 y 4, entre otras) e incluye «un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y

contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido» (STC 235/2001, de 13 de diciembre, FJ 6, y las allí citadas).

El Tribunal Constitucional ha situado dentro del concepto de seguridad pública, entre otros extremos, a «las situaciones o productos que son susceptibles de ocasionar graves riesgos para personas y bienes, lo que exige la adopción de medidas de especial intensidad», así como «la regulación de materias concretas susceptibles de originar riesgos ciertos que pueden afectar de modo directo y grave a la seguridad de personas y bienes, tomando en consideración, especialmente, fenómenos colectivos que implican la aparición de amenazas, coacciones o acciones violentas, con graves repercusiones en el funcionamiento de los servicios públicos y en la vida ciudadana» (STC 25/2004, de 26 de febrero, FJ 6).

VII

En la elaboración de este real decreto-ley se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, exigidos por el artículo 129 de la Ley 39/2015, de 1 de octubre.

Por una parte, resulta evidente el principio de proporcionalidad, toda vez que las medidas contempladas en esta norma se ajustan plenamente al objetivo que pretende conseguirse mediante este instrumento. Asimismo, cumple los principios de seguridad jurídica ya que es coherente con el resto del ordenamiento jurídico nacional y de la Unión Europea, asegurando su correcta incardinación y congruencia con la regulación vigente. Por lo demás, la norma es coherente con el principio de transparencia al haber cumplido estrictamente con los procedimientos exigidos en la tramitación de un real decreto-ley. No se han realizado los trámites de participación pública, tal y como excepciona para los reales decretos-leyes el artículo 26.11 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

Por otra parte, las medidas contenidas en el real decreto-ley son adecuadas y proporcionadas a las necesidades que exigen su dictado, sin que a estos efectos quepa considerar que existan otras alternativas menos restrictivas o que impongan menos obligaciones a los destinatarios, más bien al contrario, tras la adopción de esta norma con rango de ley se establecerán mejoras sustanciales en el ámbito de la administración electrónica, la contratación pública y las telecomunicaciones.

Se ha solicitado el informe preceptivo de la Oficina de Coordinación y Calidad Normativa, previsto en el artículo 26.9 de la Ley 59/1997, de 27 de noviembre, del Gobierno.

En su virtud, en uso de la autorización concedida en el artículo 86 de la Constitución, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, de las Ministras de Justicia, de Defensa, y de Hacienda, del Ministro del Interior, del Ministro de Política Territorial y Función Pública, por suplencia, el Ministro de Agricultura, Pesca y Alimentación, en virtud del Real Decreto 351/2019, de 20 de mayo, y de la Ministra de Economía y Empresa, y previa deliberación del Consejo de Ministros en su reunión del día 31 de octubre de 2019,

DISPONGO:

CAPÍTULO I

Medidas en materia de documentación nacional de identidad

Artículo 1. *Modificación de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.*

Se modifica el apartado 1 del artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, que queda redactado en los siguientes términos:

«1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.»

Artículo 2. *Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Se modifica el apartado 1 del artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes términos:

«1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y permite la firma electrónica de documentos.»

CAPÍTULO II

Medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas

Artículo 3. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas queda modificada en los siguientes términos:

Uno. Se modifica el apartado 2 del artículo 9, que queda con el siguiente contenido y se añade un nuevo apartado 3, renumerando el apartado 3 que pasa a ser el apartado 4:

«2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.»

Dos. Se modifica el apartado 2 del artículo 10, que queda con el siguiente contenido, y se añade un nuevo apartado 3, renumerando los apartados 3 y 4 que pasan a ser 4 y 5:

«2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la “Lista de confianza de prestadores de servicios de certificación”.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.»

Tres. Se añade una nueva disposición adicional sexta, con la siguiente redacción:

«Disposición adicional sexta. *Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).*

1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.»

Artículo 4. *Modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público queda modificada en los siguientes términos:

Uno. Se introduce un nuevo artículo 46 bis, que queda redactado como sigue:

«Artículo 46 bis. *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.»

Dos. Se da nueva redacción al artículo 155, que queda redactado como sigue:

«Artículo 155. *Transmisiones de datos entre Administraciones Públicas.*

1. De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.»

CAPÍTULO III

Medidas en materia de contratación pública

Artículo 5. *Modificación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.*

Uno. Se da nueva redacción a la letra d) del apartado 1 del artículo 35, que queda redactado como sigue:

«d) Referencia a la legislación aplicable al contrato, con expresa mención al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.»

Dos. Se introduce una nueva letra h) al apartado 2 del artículo 39, que queda con la siguiente redacción:

«h) La falta de mención en los pliegos de lo previsto en los párrafos tercero, cuarto y quinto del apartado 2 del artículo 122.»

Tres. Se da nueva redacción a la letra d) del apartado 2 del artículo 71:

«d) Haber dado lugar, por causa de la que hubiesen sido declarados culpables, a la resolución firme de cualquier contrato celebrado con una entidad de las comprendidas en el artículo 3 de la presente Ley. La prohibición alcanzará a las empresas cuyo contrato hubiere quedado resuelto por incumplimiento culpable del contratista de las obligaciones que los pliegos hubieren calificados como esenciales de acuerdo con lo previsto en el artículo 211.1.f).»

Cuatro. Se da nueva redacción al apartado 1 del artículo 116, que queda redactado como sigue:

«1. La celebración de contratos por parte de las Administraciones Públicas requerirá la previa tramitación del correspondiente expediente, que se iniciará por el órgano de contratación motivando la necesidad del contrato en los términos previstos en el artículo 28 de esta Ley y que deberá ser publicado en el perfil de contratante.

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

En aquellos contratos cuya ejecución requiera de la cesión de datos por parte de entidades del sector público al contratista, el órgano de contratación en todo caso deberá especificar en el expediente de contratación cuál será la finalidad del tratamiento de los datos que vayan a ser cedidos.»

Cinco. Se da nueva redacción al apartado 2 del artículo 122, que queda redactado como sigue:

«2. En los pliegos de cláusulas administrativas particulares se incluirán los criterios de solvencia y adjudicación del contrato; las consideraciones sociales, laborales y ambientales que como criterios de solvencia, de adjudicación o como condiciones especiales de ejecución se establezcan; los pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato; la previsión de cesión del contrato salvo en los casos en que la misma no sea posible de acuerdo con lo establecido en el segundo párrafo del artículo 214.1; la obligación del adjudicatario de cumplir las condiciones salariales de los trabajadores conforme al Convenio Colectivo sectorial de aplicación; y las demás menciones requeridas por esta Ley y sus normas de desarrollo. En el caso de contratos mixtos, se detallará el régimen jurídico aplicable a sus efectos, cumplimiento y extinción, atendiendo a las normas aplicables a las diferentes prestaciones fusionadas en ellos.

Los pliegos podrán también especificar si va a exigirse la transferencia de derechos de propiedad intelectual o industrial, sin perjuicio de lo establecido en el artículo 308 respecto de los contratos de servicios.

Los pliegos deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos.

Sin perjuicio de lo establecido en el artículo 28.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se hará constar:

- a) La finalidad para la cual se cederán dichos datos.
- b) La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.
- c) La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.
- d) La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior.
- e) La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

En los pliegos correspondientes a los contratos a que se refiere el párrafo anterior las obligaciones recogidas en las letras a) a e) anteriores en todo caso deberán ser calificadas como esenciales a los efectos de lo previsto en la letra f) del apartado 1 del artículo 211.»

Seis. Se da nueva redacción al apartado 1 del artículo 202, que queda redactado como sigue:

«1. Los órganos de contratación podrán establecer condiciones especiales en relación con la ejecución del contrato, siempre que estén vinculadas al objeto del contrato, en el sentido del artículo 145, no sean directa o indirectamente

discriminatorias, sean compatibles con el Derecho de la Unión Europea y se indiquen en el anuncio de licitación y en los pliegos.

En todo caso, será obligatorio el establecimiento en el pliego de cláusulas administrativas particulares de al menos una de las condiciones especiales de ejecución de entre las que enumera el apartado siguiente.

Asimismo en los pliegos correspondientes a los contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista será obligatorio el establecimiento de una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211.»

Siete. Se da nueva redacción al apartado 4 del artículo 215, que queda redactado como sigue:

«4. Los subcontratistas quedarán obligados solo ante el contratista principal que asumirá, por tanto, la total responsabilidad de la ejecución del contrato frente a la Administración, con arreglo estricto a los pliegos de cláusulas administrativas particulares o documento descriptivo, y a los términos del contrato; incluido el cumplimiento de las obligaciones en materia medioambiental, social o laboral a que se refiere el artículo 201, así como de la obligación a que hace referencia el último párrafo del apartado 1 del artículo 202 referida al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

El conocimiento que tenga la Administración de los subcontratos celebrados en virtud de las comunicaciones a que se refieren las letras b) y c) del apartado 2 de este artículo, o la autorización que otorgue en el supuesto previsto en la letra d) de dicho apartado, no alterarán la responsabilidad exclusiva del contratista principal.»

CAPÍTULO IV

Medidas para reforzar la seguridad en materia de telecomunicaciones

Artículo 6. *Modificación de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.*

Uno. Se da nueva redacción al apartado 6 del artículo 4, que queda redactado de la manera siguiente:

«6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de los correspondientes servicios o de la explotación de las correspondientes redes.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado,

§ 5 Real Decreto-ley de medidas urgentes por razones de seguridad pública en diversas materias

aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.»

Dos. Se introduce un nuevo apartado 3 en el artículo 6, que queda redactado como sigue:

«3. Las Administraciones Públicas deberán comunicar al Ministerio de Economía y Empresa todo proyecto de instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público, tanto si dicha instalación o explotación vaya a realizarse de manera directa, a través de cualquier entidad o sociedad dependiente de ella o a través de cualquier entidad o sociedad a la que se le haya otorgado una concesión o habilitación al efecto.

El régimen de autoprestación en la instalación o explotación de dicha red puede ser total o parcial, y por tanto dicha comunicación deberá efectuarse aun cuando la capacidad excedentaria de la citada red pueda utilizarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público.

En el caso de que se utilice o esté previsto utilizar, directamente por la administración pública o por terceros, la capacidad excedentaria de estas redes de comunicaciones electrónicas en régimen de autoprestación, el Ministerio de Economía y Empresa verificará el cumplimiento de lo previsto en el artículo 9. A tal efecto, la administración pública deberá proporcionar al Ministerio de Economía y Empresa toda la información que le sea requerida a efecto de verificar dicho cumplimiento.

La obligación establecida en este apartado se entiende sin perjuicio de la prevista en el artículo 7.3 de esta ley.»

Tres. Se da nueva redacción al apartado 15 del artículo 76, que queda redactado como sigue:

«15. El incumplimiento grave de las obligaciones en materia de acceso a redes o infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas, interconexión e interoperabilidad de los servicios.»

Cuatro. Se da nueva redacción al apartado 28 del artículo 77, que queda redactado como sigue:

«28. El incumplimiento de las obligaciones en materia de acceso a redes o infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas, interconexión e interoperabilidad de los servicios.»

Cinco. Se da nueva redacción al apartado 1 del artículo 81, que queda redactado como sigue:

«1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Economía y Empresa, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) Cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

b) Cuando exista una amenaza inmediata y grave para la salud pública.

c) Cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias.

d) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

e) Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.»

CAPÍTULO V

Medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información

Artículo 7. *Modificación del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

Se introduce un apartado 3 en el artículo 11 del siguiente tenor literal:

«3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.»

Disposición adicional única. *Comunicación de las redes de comunicaciones electrónicas en régimen de autoprestación de las Administraciones Públicas.*

Las Administraciones Públicas deberán comunicar al Ministerio de Economía y Empresa en el plazo de un mes de la entrada en vigor de este real decreto-ley las redes de comunicaciones electrónicas en régimen de autoprestación que hagan uso del dominio público a las que se refiere el artículo 6.3 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones que hayan sido instaladas o estén en proceso de instalación o explotación.

Disposición transitoria primera. *Régimen transitorio de las modificaciones introducidas en el artículo 3.*

1. Las entidades del Sector Público que quieran habilitar sistemas de identificación o firma conforme a las letras c) de los artículos 9.2 y 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a partir de la entrada en vigor de este real decreto-ley, deberán solicitar la autorización prevista en dichos preceptos. Los sistemas que, antes de la citada entrada en vigor, ya estén validados y plenamente operativos en los procedimientos administrativos de que se trate, no requerirán someterse a dicha autorización.

2. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en los artículos 9.3 y 10.3 de la Ley 39/2015, de 1 de octubre, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma.

3. En el caso de que la gestión de los recursos citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en estos artículos no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior. Los contratos adjudicados en virtud de dichos expedientes, aun cuando mantendrán su plena validez y eficacia, no podrán ser objeto de modificación que vulnere lo establecido en los citados preceptos. Tampoco podrán ser objeto de prórroga salvo que previamente sean objeto de modificación para adaptarse a

las disposiciones que en ellos se contienen, siempre y cuando ello sea posible conforme a la Ley 9/2017, de 8 de noviembre.

4. A los efectos de lo dispuesto en esta disposición transitoria se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

5. En el plazo de tres meses desde la entrada en vigor de este real decreto-ley, las distintas Administraciones Públicas remitirán a la Comisión Sectorial de Administración Electrónica la información sobre todos los contratos vigentes que tengan por objeto los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma, así como de aquellos cuyos expedientes ya estén iniciados conforme al apartado anterior.

Disposición transitoria segunda. *Régimen transitorio de las modificaciones introducidas en el artículo 4.*

1. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los sistemas de información y comunicaciones a que dicho precepto se refiere.

2. En el caso de que la gestión de los sistemas citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior.

Los contratos adjudicados en virtud de dichos expedientes, aun cuando mantendrán su plena validez y eficacia, no podrán ser objeto de modificación que vulnere lo establecido en los citados preceptos. Tampoco podrán ser objeto de prórroga salvo que previamente sean objeto de modificación para adaptarse a las disposiciones que en ellos se contienen.

3. A los efectos de lo dispuesto en esta disposición se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

Disposición transitoria tercera. *Régimen transitorio de las modificaciones introducidas en el artículo 5.*

1. Los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley se regirán por la normativa anterior. A estos efectos se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

2. No obstante lo anterior, los contratos basados en acuerdos marco que no establezcan todos los términos se regirán por la normativa vigente en la fecha de envío de la invitación a la licitación a las empresas parte del acuerdo marco o por la normativa vigente en la fecha de adjudicación si el contrato basado no requiriera una nueva licitación. En los casos en que el acuerdo marco se hubiera licitado con sujeción a la normativa anterior y, como consecuencia de la aplicación de lo dispuesto en el primer inciso de este párrafo, a alguno o algunos de los contratos basados en ese acuerdo marco le resultara de aplicación la nueva regulación resultante de este Real Decreto-ley, el órgano de contratación deberá elaborar los documentos de la licitación correspondiente a dichos contratos basados de acuerdo con esta nueva regulación.

3. El artículo 5 será de aplicación a las modificaciones de los contratos que se inicien con posterioridad a su entrada en vigor.

Disposición final primera. *Títulos competenciales.*

1. Los artículos 1 y 2 de este real decreto-ley se dictan al amparo del artículo 149.1.29.^a de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública.

2. Los artículos 3 y 4, así como las disposiciones transitoria primera y segunda se dictan al amparo del artículo 149.1.18.^a de la Constitución Española, que atribuye al Estado la competencia exclusiva para dictar las bases del régimen jurídico de las Administraciones Públicas y sobre el procedimiento administrativo común y del artículo 149.1.29.^a de la Constitución, que atribuye al Estado competencia exclusiva en materia de seguridad pública.

3. El artículo 5, así como la disposición transitoria tercera, se dictan al amparo de lo dispuesto en el artículo 149.1.18.^a de la Constitución Española en materia de bases del régimen jurídico de las Administraciones Públicas y en materia de legislación básica sobre contratos y concesiones administrativas y, en consecuencia, son de aplicación general a todas las Administraciones Públicas que entren dentro de su ámbito de aplicación, así como a los organismos y entidades dependientes de ellas.

4. El artículo 6, así como la disposición adicional única, se dictan al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21.^a de la Constitución que atribuye al Estado la competencia exclusiva en materia de régimen general de comunicaciones.

5. El artículo 7 se dicta al amparo de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.^a de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de comunicaciones y 29.^a de la Constitución, que atribuye al Estado competencia exclusiva en materia de seguridad pública.

Disposición final segunda. *Desarrollo reglamentario y ejecución.*

Se habilita al Gobierno y a las personas titulares de los departamentos ministeriales, en el ámbito de sus competencias, a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo dispuesto en este real decreto-ley.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 6

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 19 de octubre de 2022
Referencia: BOE-A-2015-10565

[...]

TÍTULO II

De la actividad de las Administraciones Públicas

CAPÍTULO I

Normas generales de actuación

Artículo 13. *Derechos de las personas en sus relaciones con las Administraciones Públicas.*

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

- a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.
- b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.
- c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.
- d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.
- e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.
- f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.
- g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.
- h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

[...]

Artículo 16. Registros.

1. Cada Administración dispondrá de un Registro Electrónico General, en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, Organismo público o Entidad vinculado o dependiente a éstos. También se podrán anotar en el mismo, la salida de los documentos oficiales dirigidos a otros órganos o particulares.

Los Organismos públicos vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende.

El Registro Electrónico General de cada Administración funcionará como un portal que facilitará el acceso a los registros electrónicos de cada Organismo. Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

Las disposiciones de creación de los registros electrónicos se publicarán en el diario oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles.

En la sede electrónica de acceso a cada registro figurará la relación actualizada de trámites que pueden iniciarse en el mismo.

2. Los asientos se anotarán respetando el orden temporal de recepción o salida de los documentos, e indicarán la fecha del día en que se produzcan. Concluido el trámite de registro, los documentos serán cursados sin dilación a sus destinatarios y a las unidades administrativas correspondientes desde el registro en que hubieran sido recibidas.

3. El registro electrónico de cada Administración u Organismo garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra. Para ello, se emitirá automáticamente un recibo consistente en una copia autenticada del documento de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro, así como un recibo acreditativo de otros documentos que, en su caso, lo acompañen, que garantice la integridad y el no repudio de los mismos.

4. Los documentos que los interesados dirijan a los órganos de las Administraciones Públicas podrán presentarse:

a) En el registro electrónico de la Administración u Organismo al que se dirijan, así como en los restantes registros electrónicos de cualquiera de los sujetos a los que se refiere el artículo 2.1.

b) En las oficinas de Correos, en la forma que reglamentariamente se establezca.

c) En las representaciones diplomáticas u oficinas consulares de España en el extranjero.

d) En las oficinas de asistencia en materia de registros.

e) En cualquier otro que establezcan las disposiciones vigentes.

Los registros electrónicos de todas y cada una de las Administraciones, deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros.

5. Los documentos presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizados, de acuerdo con lo previsto en el artículo 27 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido

presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización.

Reglamentariamente, las Administraciones podrán establecer la obligación de presentar determinados documentos por medios electrónicos para ciertos procedimientos y colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

6. Podrán hacerse efectivos mediante transferencia dirigida a la oficina pública correspondiente cualesquiera cantidades que haya que satisfacer en el momento de la presentación de documentos a las Administraciones Públicas, sin perjuicio de la posibilidad de su abono por otros medios.

7. Las Administraciones Públicas deberán hacer pública y mantener actualizada una relación de las oficinas en las que se prestará asistencia para la presentación electrónica de documentos.

8. No se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación.

Artículo 17. *Archivo de documentos.*

1. Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.

2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

[...]

Artículo 20. *Responsabilidad de la tramitación.*

1. Los titulares de las unidades administrativas y el personal al servicio de las Administraciones Públicas que tuviesen a su cargo la resolución o el despacho de los asuntos, serán responsables directos de su tramitación y adoptarán las medidas oportunas para remover los obstáculos que impidan, dificulten o retrasen el ejercicio pleno de los derechos de los interesados o el respeto a sus intereses legítimos, disponiendo lo necesario para evitar y eliminar toda anormalidad en la tramitación de procedimientos.

2. Los interesados podrán solicitar la exigencia de esa responsabilidad a la Administración Pública de que dependa el personal afectado.

[...]

Artículo 27. *Validez y eficacia de las copias realizadas por las Administraciones Públicas.*

1. Cada Administración Pública determinará los órganos que tengan atribuidas las competencias de expedición de copias auténticas de los documentos públicos administrativos o privados.

Las copias auténticas de documentos privados surten únicamente efectos administrativos. Las copias auténticas realizadas por una Administración Pública tendrán validez en las restantes Administraciones.

A estos efectos, la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante funcionario habilitado o mediante actuación administrativa automatizada.

Se deberá mantener actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la expedición de copias auténticas que deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de la citada habilitación. En este registro o sistema equivalente constarán, al menos, los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.

2. Tendrán la consideración de copia auténtica de un documento público administrativo o privado las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.

3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas:

a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

b) Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización, requerirán que el documento haya sido digitalizado y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

Se entiende por digitalización, el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento.

c) Las copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor.

d) Las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionarán mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

A estos efectos, las Administraciones harán públicos, a través de la sede electrónica correspondiente, los códigos seguros de verificación u otro sistema de verificación utilizado.

4. Los interesados podrán solicitar, en cualquier momento, la expedición de copias auténticas de los documentos públicos administrativos que hayan sido válidamente emitidos por las Administraciones Públicas. La solicitud se dirigirá al órgano que emitió el documento original, debiendo expedirse, salvo las excepciones derivadas de la aplicación de la Ley 19/2013, de 9 de diciembre, en el plazo de quince días a contar desde la recepción de la solicitud en el registro electrónico de la Administración u Organismo competente.

Asimismo, las Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo.

5. Cuando las Administraciones Públicas expidan copias auténticas electrónicas, deberá quedar expresamente así indicado en el documento de la copia.

6. La expedición de copias auténticas de documentos públicos notariales, registrales y judiciales, así como de los diarios oficiales, se regirá por su legislación específica.

Artículo 28. *Documentos aportados por los interesados al procedimiento administrativo.*

1. Los interesados deberán aportar al procedimiento administrativo los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable. Asimismo, los interesados podrán aportar cualquier otro documento que estimen conveniente.

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

4. Cuando con carácter excepcional, y de acuerdo con lo previsto en esta Ley, la Administración solicitara al interesado la presentación de un documento original y éste estuviera en formato papel, el interesado deberá obtener una copia auténtica, según los requisitos establecidos en el artículo 27, con carácter previo a su presentación electrónica. La copia electrónica resultante reflejará expresamente esta circunstancia.

5. Excepcionalmente, cuando la relevancia del documento en el procedimiento lo exija o existan dudas derivadas de la calidad de la copia, las Administraciones podrán solicitar de manera motivada el cotejo de las copias aportadas por el interesado, para lo que podrán requerir la exhibición del documento o de la información original.

6. Las copias que aporten los interesados al procedimiento administrativo tendrán eficacia, exclusivamente en el ámbito de la actividad de las Administraciones Públicas.

7. Los interesados se responsabilizarán de la veracidad de los documentos que presenten.

[. . .]

Artículo 31. *Cómputo de plazos en los registros.*

1. Cada Administración Pública publicará los días y el horario en el que deban permanecer abiertas las oficinas que prestarán asistencia para la presentación electrónica de documentos, garantizando el derecho de los interesados a ser asistidos en el uso de medios electrónicos.

2. El registro electrónico de cada Administración u Organismo se registrará a efectos de cómputo de los plazos, por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar de modo accesible y visible.

El funcionamiento del registro electrónico se registrará por las siguientes reglas:

a) Permitirá la presentación de documentos todos los días del año durante las veinticuatro horas.

b) A los efectos del cómputo de plazo fijado en días hábiles, y en lo que se refiere al cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente salvo que una norma permita expresamente la recepción en día inhábil.

Los documentos se considerarán presentados por el orden de hora efectiva en el que lo fueron en el día inhábil. Los documentos presentados en el día inhábil se reputarán anteriores, según el mismo orden, a los que lo fueran el primer día hábil posterior.

c) El inicio del cómputo de los plazos que hayan de cumplir las Administraciones Públicas vendrá determinado por la fecha y hora de presentación en el registro electrónico de cada Administración u Organismo. En todo caso, la fecha y hora efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el documento.

3. La sede electrónica del registro de cada Administración Pública u Organismo, determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla y al calendario previsto en el artículo 30.7, los días que se considerarán inhábiles a los efectos previstos en este artículo. Este será el único calendario de días inhábiles que se aplicará a efectos del cómputo de plazos en los registros electrónicos, sin que resulte de aplicación a los mismos lo dispuesto en el artículo 30.6.

[...]

TÍTULO III

De los actos administrativos

[...]

CAPÍTULO II

Eficacia de los actos

[...]

Artículo 40. *Notificación.*

1. El órgano que dicte las resoluciones y actos administrativos los notificará a los interesados cuyos derechos e intereses sean afectados por aquéllos, en los términos previstos en los artículos siguientes.

2. Toda notificación deberá ser cursada dentro del plazo de diez días a partir de la fecha en que el acto haya sido dictado, y deberá contener el texto íntegro de la resolución, con indicación de si pone fin o no a la vía administrativa, la expresión de los recursos que procedan, en su caso, en vía administrativa y judicial, el órgano ante el que hubieran de presentarse y el plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar, en su caso, cualquier otro que estimen procedente.

3. Las notificaciones que, conteniendo el texto íntegro del acto, omitiesen alguno de los demás requisitos previstos en el apartado anterior, surtirán efecto a partir de la fecha en que el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación, o interponga cualquier recurso que proceda.

4. Sin perjuicio de lo establecido en el apartado anterior, y a los solos efectos de entender cumplida la obligación de notificar dentro del plazo máximo de duración de los procedimientos, será suficiente la notificación que contenga, cuando menos, el texto íntegro de la resolución, así como el intento de notificación debidamente acreditado.

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

[...]

TÍTULO IV

De las disposiciones sobre el procedimiento administrativo común

[...]

CAPÍTULO III

Ordenación del procedimiento

Artículo 70. *Expediente Administrativo.*

1. Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

2. Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.

3. Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autenticado y acompañado de un índice, asimismo autenticado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

4. No formará parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo, como la contenida en aplicaciones, ficheros y bases de datos informáticas, notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, así como los juicios de valor emitidos por las Administraciones Públicas, salvo que se trate de informes, preceptivos y facultativos, solicitados antes de la resolución administrativa que ponga fin al procedimiento.

[...]

Disposición adicional segunda. *Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.*

Para cumplir con lo previsto en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, las Comunidades Autónomas y las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En el caso que una Comunidad Autónoma o una Entidad Local justifique ante el Ministerio de Hacienda y Administraciones Públicas que puede prestar el servicio de un modo más eficiente, de acuerdo con los criterios previstos en el párrafo anterior, y opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas.

Téngase en cuenta que se declara que el párrafo segundo no es inconstitucional interpretado en los términos del fundamento jurídico 11 f) por Sentencia del TC 55/2018, de 24 de mayo. Ref. [BOE-A-2018-8574](#)

[...]

Disposición adicional octava. *Resoluciones de Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital que establezcan las condiciones de uso de sistemas de identificación y/o firma no criptográfica.*

Cuando se trate de sistemas establecidos por medio de Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital para su ámbito competencial con objeto de determinar las circunstancias en las que un sistema de firma electrónica no basado en certificados electrónicos será considerado como válido en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado, sus organismos públicos y entidades de Derecho Público vinculados o dependientes, no será preciso el transcurso del plazo de dos meses para la eficacia jurídica del sistema a que se refiere el artículo 10.2.c) de la presente ley, adquiriendo eficacia jurídica al día siguiente de la publicación de la Resolución, salvo que esta disponga otra cosa.

[...]

§ 7

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras

Agencia Española de Protección de Datos
«BOE» núm. 296, de 12 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-21648

El incremento que últimamente están experimentando las instalaciones de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Además es un sector que ofrece múltiples medios de tratar datos personales como pueden ser los circuitos cerrados de televisión, grabación por dispositivos «webcam», digitalización de imágenes o instalación de cámaras en el lugar de trabajo. Precisamente la última Conferencia Internacional de Autoridades de Protección de Datos, celebrada en Londres los pasados días 1 a 3 de noviembre de este año, ha girado en torno a la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos. Todo esto hace necesario que, en ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1332/1994 de 20 de junio, que considera como dato de carácter personal la información gráfica o fotográfica.

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

§ 7 Tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

Se excluyen de la presente Instrucción los datos personales grabados para uso o finalidad doméstica de conformidad con lo establecido en el artículo 2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, si bien en el sentido estricto señalado por el Tribunal de Justicia de las Comunidades Europeas en la Sentencia de 6 de noviembre de 2003, asunto Lindqvist, que al interpretar la excepción prevista en el artículo 3 apartado 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, indica que únicamente contempla «las actividades que se inscriben en el marco de la vida privada o familiar de los particulares» y no otras distintas. En la misma línea se pronuncia el Dictamen 4/2004, adoptado por el Grupo de Trabajo creado por el Artículo 29 de la Directiva 95/46/CE, con fecha 25 de noviembre de 2002.

Además, la Instrucción tampoco se aplicará al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad, que está cubierto por normas específicas, aunque estos tratamientos también deberán cumplir las garantías establecidas por la Ley Orgánica 15/1999.

Por otro lado, la Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta materia han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE.

Por último, las plenas garantías de protección de los datos personales, así como las peculiaridades de su tratamiento exige una regulación concreta evitando la aplicación de un conjunto de reglas abstractas y dispersas. Por ello, a la hora de regular la legitimación del tratamiento de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente. Asimismo se regula el contenido del deber de información previsto en el artículo 5 de la misma Ley Orgánica, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Por descontado, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

En su virtud, de conformidad con lo dispuesto en el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dispongo:

Artículo 1. *Ámbito objetivo.*

1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.

2. El tratamiento de los datos personales procedentes de las imágenes obtenidas mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad se regirá por las disposiciones sobre la materia.

3. No se considera objeto de regulación de esta Instrucción el tratamiento de imágenes en el ámbito personal y doméstico, entendiéndose por tal el realizado por una persona física en el marco de una actividad exclusivamente privada o familiar.

Artículo 2. *Legitimación.*

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.

Artículo 3. *Información.*

Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

- a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y
- b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.

Artículo 4. *Principios de calidad, proporcionalidad y finalidad del tratamiento.*

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

Artículo 5. Derechos de las personas.

1. Para el ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, el/la afectado/a deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. El ejercicio de estos derechos se llevará a cabo de conformidad con lo dispuesto en la citada Ley Orgánica y su normativa de desarrollo.

2. El responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento.

3. El/la interesado/a al que se deniegue total o parcialmente el ejercicio de los derechos señalados en el párrafo anterior, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos.

Artículo 6. Cancelación.

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

Artículo 7. Notificación de ficheros.

1. La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Artículo 8. Seguridad y Secreto.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.

Disposición transitoria.

Los responsables de ficheros de videovigilancia ya inscritos en el Registro General de la Agencia Española de Protección de Datos deberán adoptar las medidas previstas en el artículo 3, letra a), y en el artículo 4.3 de esta Instrucción en el plazo máximo de tres meses desde su entrada en vigor.

Disposición final.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

§ 7 Tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras

2. El modelo a que se refiere el apartado anterior, está disponible en la página web de la Agencia Española de Protección de Datos, www.agpd.es, de donde podrá ser descargado, especificando los datos del responsable.

§ 8

Resolución de 9 de marzo de 2016, de la Presidencia de la Comisión Nacional de los Mercados y la Competencia, por la que se crea el fichero de datos de carácter personal "Registro de grupos de interés"

Comisión Nacional de los Mercados y la Competencia
«BOE» núm. 61, de 11 de marzo de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-2488

El artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), establece que la creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o en el Diario Oficial correspondiente. Por su parte, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD (RLOPD) dispone que la disposición o acuerdo de creación, modificación o supresión deberá revestir la forma de orden ministerial o resolución del titular de la entidad, y detalla los extremos que deberán precisarse.

En cumplimiento de la disposición antes citada, la Comisión Nacional de los Mercados y la Competencia dictó Resolución, de 3 de noviembre de 2014 (BOE de 12 de diciembre de 2014), por la que se crean, modifican y suprimen ficheros automatizados de datos de carácter personal en este organismo.

Por otra parte, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, establece que el sistema de tratamiento de los ficheros de datos de carácter personal debe figurar en las disposiciones pertinentes que regulan tales ficheros.

La adopción de la presente Resolución obedece a la necesidad de dar de alta un fichero automatizado de datos de carácter personal e inscribirlo en la Agencia Española de Protección de Datos, creado en virtud de la Resolución del Presidente de la Comisión Nacional de los Mercados y la Competencia de 26 de febrero de 2016, y obedeciendo a las siguientes finalidades: reforzar la transparencia de actuación y las obligaciones de buen gobierno de la Comisión, en los términos que propugnan la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, como elementos que refuerzan la legitimidad de la propia Comisión y que infunden confianza a los ciudadanos respecto de la Comisión y su actividad.

En el ejercicio de las atribuciones conferidas por el artículo 19.1.c) y p) de la Ley 3/2013, de 4 de junio, de creación de la CNMC, y el artículo 15.2.p) del Real Decreto 657/2013, de 30 de agosto, por el que se aprueba el Estatuto Orgánico de la CNMC, y a fin de dar cumplimiento al mandato legal del artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, sobre creación de ficheros automatizados que contengan datos de carácter

§ 8 Creación del fichero de datos de carácter personal "Registro de grupos de interés"

personal gestionados por la Comisión Nacional de los Mercados y la Competencia, y asegurar a los administrados el ejercicio legítimo de sus derechos,

El Presidente de la Comisión Nacional de los Mercados y la Competencia ha dispuesto:

Primero.

De conformidad con lo previsto en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, y a los efectos previstos en el mismo, crear el fichero automatizado de la Comisión Nacional de los Mercados y la Competencia que contiene y procesa los datos de carácter personal que se relacionan y describen en el anexo I.

Segundo.

El titular del órgano responsable del citado fichero adoptará las medidas de gestión y organización que sean necesarias, asegurando, en todo caso, la confidencialidad, seguridad e integridad de los datos, así como las conducentes a hacer efectivas las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y sus normas de desarrollo.

Tercero.

La presente Resolución entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Creación de ficheros

Fichero: «Registro de grupos de interés de la CNMC»

a) Finalidad del fichero y usos previstos del mismo: Sistema de información que da soporte al Registro de grupos de interés de la CNMC.

b) Personas sobre las que se pretende obtener datos o que resultan obligadas a suministrarlos: El propio interesado (persona física o jurídica) o su representante legal o personas de contacto de grupos de interés.

c) Procedimiento de recogida de datos de carácter personal y procedencia de los mismos: Los datos son facilitados voluntariamente por los propios sujetos mediante declaraciones y/o formularios en soporte papel o electrónico al efecto.

d) Estructura básica del fichero automatizado y descripción de los tipos de datos de carácter personal incluidos en el mismo: La estructura básica de este fichero está constituida por varias tablas en la que se recogen los siguientes datos identificativos de los usuarios de la aplicación: personales (nombre y apellidos del interesado, su representante legal o persona de contacto, empresa, NIF o documento equivalente, domicilio social y/o dirección postal completa, teléfono y fax profesionales, firma, firma electrónica y correo electrónico, página web); profesionales (puesto o representación); otros (finalidad y objetivos, actividades específicas y ámbitos de interés).

e) Sistema de tratamiento: Mixto.

f) Comunicaciones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros: Además del acceso público a través de consulta en internet, con carácter general, no se prevé la comunicación de estos datos en términos distintos a los indicados ni la transferencia a países terceros.

g) Órgano responsable de este fichero: Comisión Nacional de los Mercados y la Competencia. Presidencia de la Comisión Nacional de los Mercados y la Competencia, calle Alcalá, 47, 28014 Madrid. Teléfono: 91 432 96 00.

h) Servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Presidencia de la Comisión Nacional de los Mercados y la Competencia, calle Alcalá, 47, 28014 Madrid. Teléfono: 91 432 96 00.

i) Medidas de seguridad con indicación del nivel: Las medidas de seguridad que se aplican son las definidas para el nivel básico en el título VIII del RLOPD.

§ 9

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Jefatura del Estado
«BOE» núm. 218, de 8 de septiembre de 2018
Última modificación: 30 de marzo de 2022
Referencia: BOE-A-2018-12257

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.

El carácter transversal e interconectado de las tecnologías de la información y de la comunicación, que también caracteriza a sus amenazas y riesgos, limita la eficacia de las medidas que se emplean para contrarrestarlos cuando se toman de modo aislado. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos sectoriales afectados.

Por tanto, es oportuno establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

II

Con este propósito se dicta este real decreto-ley, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. El real decreto-ley se apoya igualmente en las normas, en los instrumentos de respuesta a incidentes y en los órganos de coordinación estatal existentes en esta materia, lo que, junto a las razones señaladas en el apartado I, justifica que su contenido trascienda el de la propia Directiva.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

El real decreto-ley se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Su ámbito de aplicación se extiende a sectores que no están expresamente incluidos en la Directiva, para darle a este real decreto-ley un enfoque global, aunque se preserva su legislación específica. Adicionalmente, en el caso de las actividades de explotación de las redes y de prestación de servicios de comunicaciones electrónicas y los recursos asociados, así como de los servicios electrónicos de confianza, expresamente excluidos de dicha Directiva, el real decreto-ley se aplicará únicamente en lo que respecta a los operadores críticos.

El real decreto-ley se aplicará, así mismo, a los proveedores de determinados servicios digitales. La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los somete a un régimen de armonización máxima, equivalente a un reglamento, pues se considera que su regulación a escala nacional no sería efectiva por tener un carácter intrínsecamente transnacional. La función de las autoridades nacionales se limita, por tanto, a supervisar su aplicación por los proveedores establecidos en su país, y coordinarse con las autoridades correspondientes de otros países de la Unión Europea.

Siguiendo la citada Directiva, el real decreto-ley identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios, que son, en definitiva, los destinatarios de este real decreto-ley.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilicen, aunque su gestión esté externalizada. Las obligaciones de seguridad que asuman deberán ser proporcionadas al nivel de riesgo que afronten y estar basadas en una evaluación previa de los mismos. Las normas de desarrollo de este real decreto-ley podrán concretar las obligaciones de seguridad exigibles a los operadores de servicios esenciales, incluyendo en su caso las inspecciones a realizar o la participación en actividades y ejercicios de gestión de crisis.

El real decreto-ley requiere así mismo que los operadores de servicios esenciales y los proveedores de servicios digitales notifiquen los incidentes que sufran en las redes y servicios de información que emplean para la prestación de los servicios esenciales y digitales, y tengan efectos perturbadores significativos en los mismos, al tiempo que prevé la notificación de los sucesos o incidencias que puedan afectar a los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquellos, y perfila los procedimientos de notificación.

La notificación de incidentes forma parte de la cultura de gestión de riesgos que la Directiva y el real decreto-ley fomentan. Por ello, el real decreto-ley protege a la entidad notificante y al personal que informe sobre incidentes ocurridos; se reserva la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permite la notificación de incidentes cuando no sea obligada su comunicación.

El real decreto-ley recalca la necesidad de tener en cuenta los estándares europeos e internacionales, así como las recomendaciones que emanen del grupo de cooperación y de la red de CSIRT (Computer Security Incident Response Team) establecidos en el ámbito comunitario por la Directiva, con vistas a aplicar las mejores prácticas aprendidas en estos foros y contribuir al impulso del mercado interior y a la participación de nuestras empresas en él.

Con el fin de aumentar su eficacia y, al tiempo, reducir las cargas administrativas y económicas que estas obligaciones suponen para las entidades afectadas, este real decreto-ley trata de garantizar su coherencia con las que se derivan de la aplicación de otras normativas en materia de seguridad de la información, tanto de carácter horizontal como sectorial, y la coordinación en su aplicación con las autoridades responsables en cada caso.

Respecto a las normas horizontales, destacan los vínculos establecidos con las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, y con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

en el ámbito de la Administración Electrónica, como normativa especial en materia de seguridad de los sistemas de información del sector público.

Así, se aproxima el ámbito de aplicación de este real decreto-ley al de la Ley 8/2011, de 28 de abril, añadiendo a los sectores previstos por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los sectores estratégicos adicionales contemplados en esa ley; se apoya en ella para definir el concepto de «servicio esencial», y se atribuye a sus órganos colegiados la determinación de los servicios esenciales y de los operadores de servicios esenciales sujetos al presente real decreto-ley. Teniendo en cuenta la Ley 36/2015, de 28 de septiembre, se atribuye al Consejo de Seguridad Nacional la función de actuar como punto de contacto con otros países de la Unión Europea y un papel coordinador de la política de ciberseguridad a través de la Estrategia de Ciberseguridad Nacional.

III

La Estrategia de Ciberseguridad Nacional con la que España cuenta desde el año 2013, sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. Dicha Estrategia seguirá desarrollando el marco institucional de la ciberseguridad que este real decreto-ley esboza, compuesto por las autoridades públicas competentes y los CSIRT de referencia, por una parte, y la cooperación público-privada, por otra.

Las autoridades competentes ejercerán las funciones de vigilancia derivadas de este real decreto-ley y aplicarán el régimen sancionador cuando proceda. Así mismo, promoverán el desarrollo de las obligaciones que el real decreto-ley impone, en consulta con el sector y con las autoridades que ejerzan competencias por razón de la materia cuando se refieran a sectores específicos, para evitar la existencia de obligaciones duplicadas, innecesarias o excesivamente onerosas.

Los CSIRT son los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT (Computer Emergency Response Team), registrado en EE.UU.

El real decreto-ley delimita el ámbito funcional de actuación de los CSIRT de referencia previstos en ella. Dichos CSIRT son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a ellos, pero el destinatario de las notificaciones es la autoridad competente respectiva, que tendrá en cuenta esta información para la supervisión de los operadores. En todo caso, el operador es responsable de resolver los incidentes y reponer las redes y sistemas de información afectados a su funcionamiento ordinario.

Se prevé la utilización de una plataforma común para la notificación de incidentes, de tal manera que los operadores no deban efectuar varias notificaciones en función de la autoridad a la que deban dirigirse. Esta plataforma podrá ser empleada también para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

IV

Este real decreto-ley consta de siete títulos que contienen, en primer lugar, las definiciones de los términos que se usan a lo largo del texto, la salvaguarda de funciones estatales esenciales, como la seguridad nacional y otras disposiciones generales. A continuación, en el título II se determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten a los que se aplicará el real decreto-ley. El orden en que se procederá a su identificación por primera vez se establece en la disposición adicional primera del real decreto-ley. El título III recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información que se ha descrito anteriormente. Se dedica un precepto específico a la cooperación entre autoridades públicas, como pilar de un ejercicio adecuado de las diferentes competencias concurrentes sobre la materia.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

El título IV se ocupa de las obligaciones de seguridad de los operadores, y en él se prevé la aplicación preferente de normas sectoriales que impongan obligaciones equivalentes a las previstas en este real decreto-ley, sin perjuicio de la coordinación ejercida por el Consejo de Seguridad Nacional y del deber de cooperación con las autoridades competentes en virtud de este real decreto-ley.

En el título V, el más extenso, se regula la notificación de incidentes y se presta atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión. En el título VI, se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, y en el título VII se tipifican las infracciones y sanciones de este real decreto-ley. En este aspecto, el real decreto-ley se decanta por impulsar la subsanación de la infracción antes que su castigo, el cual, si es necesario dispensarlo, será efectivo, proporcionado y disuasorio, en línea con lo ordenado por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

El real decreto-ley se cierra con una parte final que incluye las disposiciones adicionales y finales necesarias para completar la regulación.

Esta disposición ha sido sometida al procedimiento de información de normas reglamentarias técnicas y de reglamentos relativos a los servicios de la sociedad de la información, previsto en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, así como el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información. Así mismo, se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa, como son los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública por el artículo 149.1.21.^a y 29.^a de la Constitución.

El real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (Sentencias 6/1983, de 4 de febrero, F. 5; 11/2002, de 17 de enero, F. 4, 137/2003, de 3 de julio, F. 3 y 189/2005, de 7 julio, F.3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever requiere una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las Leyes.

Por otro lado, la utilización del instrumento jurídico del real decreto-ley, en el presente caso, además queda justificada por la doctrina del Tribunal Constitucional, que, en su Sentencia 1/2012, de 13 de enero, ha avalado la concurrencia del presupuesto habilitante de la extraordinaria y urgente necesidad del artículo 86.1 de la Constitución, cuando concurra el retraso en la transposición de directivas.

En efecto, el plazo de transposición de la mencionada Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se encuentra ya vencido a 9 de mayo de 2018. La finalización del plazo de transposición de esta Directiva ha motivado la iniciación por parte de la Comisión Europea de un procedimiento formal de infracción n.º 2018/168.

En consecuencia, se entiende que en el conjunto y en cada una de las medidas que se adoptan mediante el real decreto-ley proyectado, concurren, por su naturaleza y finalidad, las circunstancias de extraordinaria y urgente necesidad que exige el artículo 86 de la Constitución como presupuestos habilitantes para la aprobación de un real decreto-ley.

En su virtud, haciendo uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, del Ministro del Interior y de la Ministra

de Economía y Empresa y previa deliberación del Consejo de Ministros, en su reunión del día 7 de septiembre de 2018,

DISPONGO:

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

Artículo 2. *Ámbito de aplicación.*

1. Este real decreto-ley se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto-ley:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3. Este real decreto-ley no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

Artículo 3. *Definiciones.*

A los efectos de este real decreto-ley, se entenderá por:

a) Redes y sistemas de información, cualquiera de los elementos siguientes:

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

1.º Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales;

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

b) Seguridad de las redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

d) Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.

h) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

i) Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

j) Representante: persona física o jurídica establecida en la Unión Europea que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea, a la que, en sustitución del proveedor de servicios digitales, pueda dirigirse una autoridad competente nacional o un CSIRT, en relación con las obligaciones que, en virtud de este real decreto-ley, tiene el proveedor de servicios digitales.

k) Norma técnica: una norma en el sentido del artículo 2.1 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

l) Especificación: una especificación técnica en el sentido del artículo 2.4 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012.

m) Punto de intercambio de Internet («IXP», por sus siglas en inglés de «Internet eXchange Point»): una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet. Un IXP permite interconectar sistemas autónomos sin requerir que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

n) Sistema de nombres de dominio («DNS», por sus siglas en inglés de «Domain Name System»): sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en Internet.

o) Proveedor de servicios de DNS: entidad que presta servicios de DNS en Internet.

p) Registro de nombres de dominio de primer nivel: entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

q) Mercado en línea: servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en un sitio web específico del servicio de mercado en línea, o en un sitio web de un empresario que utilice servicios informáticos proporcionados al efecto por el proveedor del servicio de mercado en línea.

r) Motor de búsqueda en línea: servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

Artículo 4. *Directrices y orientaciones comunitarias.*

En la aplicación de este real decreto-ley y en la elaboración de los reglamentos y guías previstos en él se tendrán en cuenta los actos de ejecución de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, así como todas las recomendaciones y directrices emanadas del grupo de cooperación establecido por el artículo 11 de la citada Directiva, y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquella.

Artículo 5. *Salvaguarda de funciones estatales esenciales.*

Lo dispuesto en este real decreto-ley se entenderá sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores.

TÍTULO II

Servicios esenciales y servicios digitales

Artículo 6. *Identificación de servicios esenciales y de operadores de servicios esenciales.*

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Se identificará a un operador como operador de servicios esenciales si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:

a) En relación con la importancia del servicio prestado:

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial;

2.º La valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública.

b) En relación con los clientes de la entidad evaluada:

- 1.º El número de usuarios que confían en los servicios prestados por ella;
- 2.º Su cuota de mercado.

Reglamentariamente podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.

2. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.

3. En la identificación de los servicios esenciales y de los operadores de servicios esenciales se tendrán en consideración, en la mayor medida posible, las recomendaciones pertinentes que adopte el grupo de cooperación.

4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos de contacto único de dichos Estados sobre la intención de identificarlo como operador de servicios esenciales.

Artículo 7. *Comunicación de actividad por los proveedores de servicios digitales.*

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

TÍTULO III

Marco estratégico e institucional

Artículo 8. *Marco estratégico de seguridad de las redes y sistemas de información.*

La Estrategia de Ciberseguridad Nacional, al amparo y alineada con la Estrategia de Seguridad Nacional, enmarca los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.

La Estrategia de Ciberseguridad Nacional abordará, entre otras cuestiones, las establecidas en el artículo 7 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

A tal efecto, el Consejo de Seguridad Nacional impulsará la revisión de la Estrategia de Ciberseguridad Nacional, de conformidad con lo dispuesto en el artículo 21.1 e) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 9. *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

2.º En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.

b) Para los proveedores de servicios digitales: la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

Artículo 10. *Funciones de las autoridades competentes.*

Las autoridades competentes ejercerán las siguientes funciones:

a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.

b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.

c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.

d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de este real decreto-ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.

e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de este real decreto-ley, conforme a lo establecido en el artículo 27.

f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 26.

g) Cooperar, en el ámbito de aplicación de este real decreto-ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes, conforme a lo establecido en los artículos 14 y 29.

h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 16 y 19.

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 17.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 25.

Artículo 11. *Equipos de respuesta a incidentes de seguridad informática de referencia.*

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

Artículo 12. *Requisitos y funciones de los CSIRT de referencia.*

1. Los CSIRT deberán reunir las siguientes condiciones:

a) Garantizarán un elevado nivel de disponibilidad de sus servicios de comunicaciones evitando los fallos ocasionales y contarán con varios medios para que se les pueda contactar y puedan contactar a otros en todo momento. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos de los grupos de usuarios y los socios colaboradores.

b) Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros.

c) Garantizarán la continuidad de las actividades. Para ello:

1.º Estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.

2.º Contarán con personal suficiente para garantizar su disponibilidad en todo momento.

3.º Tendrán acceso a infraestructuras de comunicación cuya continuidad esté asegurada. A tal fin, dispondrán de sistemas redundantes y espacios de trabajo de reserva.

d) Deberán tener la capacidad de participar, cuando lo deseen, en redes de cooperación internacional.

2. Los CSIRT desempeñarán como mínimo, las siguientes funciones:

a) Supervisar incidentes a escala nacional.

b) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados.

c) Responder a incidentes.

d) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

e) Participar en la red de CSIRT.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

3. Los CSIRT establecerán relaciones de cooperación con el sector privado. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas de:

- a) Procedimientos de gestión de incidentes y riesgos.
- b) Sistemas de clasificación de incidentes, riesgos e información.

Artículo 13. *Punto de contacto único.*

El Consejo de Seguridad Nacional ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Artículo 14. *Cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales.*

1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.

2. Consultarán así mismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de este real decreto-ley, y colaborarán con ellos en el ejercicio de sus funciones.

3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello.

Artículo 15. *Confidencialidad de la información sensible.*

Sin perjuicio de lo dispuesto en el artículo 5, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, así como la confidencialidad de la información que recaben de éstos en el ejercicio de las funciones que les encomienda el presente real decreto-ley.

Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

TÍTULO IV

Obligaciones de seguridad

Artículo 16. *Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley.

Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.

2. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.

3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.

Sus funciones específicas serán las previstas reglamentariamente.

4. Las autoridades competentes podrán establecer mediante Orden ministerial obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información, a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia, en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia, con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

6. Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos:

- a) La seguridad de los sistemas e instalaciones;
- b) La gestión de incidentes;
- c) La gestión de la continuidad de las actividades;
- d) La supervisión, auditorías y pruebas;
- e) El cumplimiento de las normas internacionales.

Los proveedores de servicios digitales atenderán igualmente a los actos de ejecución por los que la Comisión europea detalle los aspectos citados.

7. Los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público que utilizan servicios ofrecidos por proveedores de servicios digitales, en particular servicios de computación en nube, podrán exigir a los proveedores de tales servicios medidas de seguridad adicionales, más estrictas que las que dichos proveedores han adoptado en cumplimiento de la legislación en materia de seguridad de las redes y sistemas de información. En particular, las citadas medidas podrán ser exigidas mediante obligaciones contractuales, previo informe preceptivo y vinculante del Centro Criptológico Nacional.

Artículo 17. *Normas técnicas.*

Las autoridades competentes promoverán la utilización de regulaciones, normas o especificaciones técnicas en materia de seguridad de las redes y sistemas de información elaboradas en el marco del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea.

En ausencia de dichas normas o especificaciones, promoverán la aplicación de las normas o recomendaciones internacionales aprobadas por los organismos internacionales de normalización, y, en su caso, de las normas y especificaciones técnicas aceptadas a nivel europeo o internacional que sean pertinentes en esta materia.

Artículo 18. *Sectores con normativa específica equivalente.*

Cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en este real decreto-ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

Ello no afectará al deber de cooperación entre autoridades competentes, a la coordinación ejercida por el Consejo de Seguridad Nacional ni, en la medida en que no sea incompatible con la legislación sectorial, a la aplicación del título V sobre notificación de incidentes.

TÍTULO V

Notificación de incidentes

Artículo 19. *Obligación de notificar.*

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios.

Las notificaciones podrán referirse también, conforme se determine reglamentariamente, a los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquéllos.

2. Así mismo, los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.

La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente.

3. Las notificaciones tanto de operadores de servicios esenciales como de proveedores de servicios digitales se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos, incluso si éstos son proveedores de servicios digitales sometidos a este real decreto-ley.

4. Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

5. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer, mediante Orden ministerial, obligaciones específicas de notificación por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de notificación de incidentes a los que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

6. La obligación de notificación de incidentes prevista en los apartados anteriores no obsta al cumplimiento de los deberes legales de denuncia de aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal y teniendo en cuenta lo previsto en el artículo 14.3 de este real decreto-ley.

Artículo 20. *Protección del notificante.*

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

Artículo 21. *Factores para determinar la importancia de los efectos de un incidente.*

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

- a) El número de usuarios afectados por la perturbación del servicio esencial.
- b) La duración del incidente.
- c) La extensión o áreas geográficas afectadas por el incidente.
- d) El grado de perturbación del funcionamiento del servicio.
- e) El alcance del impacto en actividades económicas y sociales cruciales.
- f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.
- g) El daño a la reputación.

2. En las notificaciones a las que se refiere el artículo 19.2, la importancia de un incidente se determinará conforme a lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

Artículo 22. *Notificación inicial, notificaciones intermedias y notificación final.*

1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 19.1 sin dilación indebida.

La notificación incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.

2. Los operadores de servicios esenciales efectuarán las notificaciones intermedias que sean precisas para actualizar la información incorporada a la notificación inicial e informar sobre la evolución del incidente, mientras éste no esté resuelto.

3. Los operadores de servicios esenciales enviarán una notificación final del incidente tras su resolución.

Un incidente se considerará resuelto cuando se hayan restablecido las redes y sistemas de información afectados y el servicio opere con normalidad.

Artículo 23. *Flexibilidad en la observancia de los plazos para la notificación.*

Los operadores de servicios esenciales y los proveedores de servicios digitales podrán omitir, en las comunicaciones que realicen sobre los incidentes que les afecten, la información de la que aún no dispongan relativa a su repercusión sobre servicios esenciales u otros servicios que dependan de ellos para su prestación, u otra información de la que no dispongan. Tan pronto como conozcan dicha información deberán remitirla a la autoridad competente.

Si, transcurrido un tiempo prudencial desde la notificación inicial del incidente, el operador de servicios esenciales o el proveedor de servicios digitales no hubiera podido reunir la información pertinente, enviará a la autoridad competente, sin demora, un informe justificativo de las actuaciones realizadas para reunir la información y de los motivos por los que no ha sido posible obtenerla.

Artículo 24. *Incidentes que afecten a servicios digitales.*

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este real decreto-ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que estuviese establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o de notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.

Artículo 25. *Tramitación de incidentes con impacto transfronterizo.*

1. Cuando las autoridades competentes o los CSIRT de referencia tengan noticia de incidentes que pueden afectar a otros Estados miembros de la Unión Europea, informarán a través del punto de contacto único a los Estados miembros afectados, precisando si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en dichos Estados.

2. Cuando a través de dicho punto de contacto se reciba información sobre incidentes notificados en otros países de la Unión Europea que puedan tener efectos perturbadores significativos para los servicios esenciales prestados en España, se remitirá la información relevante a la autoridad competente y al CSIRT de referencia, para que adopten las medidas pertinentes en el ejercicio de sus funciones respectivas.

3. Las actuaciones consideradas en los apartados anteriores se entienden sin perjuicio de los intercambios de información que las autoridades competentes o los CSIRT de referencia puedan realizar de modo directo con sus homólogos de otros Estados miembros de la Unión Europea en relación con aquellos incidentes que puedan resultar de interés mutuo.

Artículo 26. *Información al público.*

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.

Artículo 27. *Información anual al punto de contacto único y al grupo de cooperación.*

1. Las autoridades competentes transmitirán al punto de contacto único un informe anual sobre el número y tipo de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea.

Las autoridades competentes elaborarán el informe siguiendo las instrucciones que dicte el punto de contacto único teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

2. El punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año un informe anual resumido sobre las notificaciones recibidas, y lo remitirá ulteriormente a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

Artículo 28. *Obligación de resolver los incidentes, de información y de colaboración mutua.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.

En tales casos deberán atender a las indicaciones que reciban del CSIRT de referencia para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales han de suministrar al CSIRT de referencia y a la autoridad competente toda la información que se les requiera para el desempeño de las funciones que les encomienda el presente real decreto-ley.

En particular, podrá requerirse información adicional a los operadores de servicios esenciales y a los proveedores de servicios digitales para analizar la naturaleza, causas y efectos de los incidentes notificados, y para elaborar estadísticas y reunir los datos necesarios para elaborar los informes anuales considerados en el artículo 27.

Cuando las circunstancias lo permitan, la autoridad competente o el CSIRT de referencia proporcionarán a los operadores de servicios esenciales o a los proveedores de servicios digitales afectados por incidentes la información derivada de su seguimiento que pueda serles relevante, en particular, para resolver el incidente.

Artículo 29. *Cooperación en lo relativo a los incidentes que afecten a datos personales.*

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.

Artículo 30. *Autorización para la cesión de datos personales.*

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

Su cesión para estos fines se entenderá autorizada en los siguientes casos:

- a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.
- b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.
- c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.
- d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.
- e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

Artículo 31. *Notificaciones voluntarias.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales podrán notificar los incidentes para los que no se establezca una obligación de notificación.

Así mismo, las entidades que presten servicios esenciales y no hayan sido identificadas como operadores de servicios esenciales y que no sean proveedores de servicios digitales podrán notificar los incidentes que afecten a dichos servicios.

Estas notificaciones obligan a la entidad que las efectúe a resolver el incidente de acuerdo con lo establecido en el artículo 28.

2. Las notificaciones a las que se refiere el apartado anterior se registrarán por lo dispuesto en este título, y se informará sobre ellas al punto de contacto único en el informe anual previsto en el artículo 27.1.

3. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los CSIRT y por las autoridades competentes.

TÍTULO VI

Supervisión

Artículo 32. *Supervisión de los operadores de servicios esenciales.*

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá requerir al operador que subsane las deficiencias detectadas e indicarle cómo debe hacerlo.

Artículo 33. *Supervisión de los proveedores de servicios digitales.*

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de este real decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia.

En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

2. Cuando la autoridad competente tenga noticia de incidentes que perturben de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medidas de supervisión pertinentes.

A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

Artículo 34. *Cooperación transfronteriza.*

1. La supervisión se llevará a cabo, cuando proceda, en cooperación con las autoridades competentes de los Estados miembros en los que se ubiquen las redes y sistemas de información empleados para la prestación del servicio, o en que esté establecido el operador de servicios esenciales, el proveedor de servicios digitales o su representante.

2. Las autoridades competentes colaborarán con las autoridades competentes de otros Estados miembros cuando éstas requieran su cooperación en la supervisión y adopción de medidas por operadores de servicios esenciales y proveedores de servicios digitales en relación con las redes y sistemas de información ubicados en España, así como respecto a los proveedores de servicios digitales establecidos en España o cuyo representante en la Unión Europea tenga su residencia o domicilio social en España.

TÍTULO VII

Régimen sancionador

Artículo 35. *Responsables.*

Serán responsables los operadores de servicios esenciales y los proveedores de servicios digitales comprendidos en el ámbito de aplicación de este real decreto-ley.

Artículo 36. *Infracciones.*

1. Las infracciones de los preceptos de este real decreto-ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La falta de adopción de medidas para subsanar las deficiencias detectadas, de acuerdo con lo dispuesto en los artículos 32.2 o 33.1, cuando éstas le hayan hecho vulnerable a un incidente con efectos perturbadores significativos en el servicio y el operador de servicios esenciales o el proveedor de servicios digitales no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.

b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio. Se considerará que es reiterado a partir del segundo incumplimiento.

c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un efecto perturbador significativo en la prestación servicios esenciales o de servicios digitales en España o en otros Estados miembros.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

3. Son infracciones graves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente referidas a las precauciones mínimas que los operadores de servicios esenciales han de adoptar para garantizar la seguridad de las redes y sistemas de información.

b) La falta de adopción de medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento dictado de acuerdo con los artículos 32.2 o 33.1, cuando ese sea el tercer requerimiento desatendido que se dicta en los cinco últimos años.

c) El incumplimiento de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

d) La demostración de una notoria falta de interés en la resolución de incidentes con efectos perturbadores significativos notificados cuando dé lugar a una mayor degradación del servicio.

e) Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.

f) Poner obstáculos a la realización de auditorías por la autoridad competente.

4. Son infracciones leves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente al amparo de este real decreto-ley, cuando no suponga una infracción grave.

b) La falta de adopción de medidas para corregir las deficiencias detectadas en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 o 33.1.

c) No facilitar la información que sea requerida por las autoridades competentes sobre sus políticas de seguridad, o proporcionar información incompleta o tardía sin justificación.

d) No someterse a una auditoría de seguridad según lo ordenado por la autoridad competente.

e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten en virtud del artículo 28.2.

f) La falta de notificación de los sucesos o incidencias para los que, aunque no hayan tenido un efecto adverso real sobre los servicios, exista obligación de notificación en virtud del párrafo segundo del artículo 19.2.

g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 23, o no remitir el informe justificativo sobre la imposibilidad de reunir la información previsto en dicho artículo.

h) No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente, de acuerdo con el artículo 28.

Artículo 37. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.

b) Por la comisión de infracciones graves, multa de 100.001 hasta 500.000 euros.

c) Por la comisión de infracciones leves, amonestación o multa hasta 100.000 euros.

2. Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el sitio de Internet de la autoridad competente, en atención a los hechos concurrentes y de conformidad con el artículo siguiente.

Artículo 38. Graduación de la cuantía de las sanciones.

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

- d) La reincidencia, por comisión en el último año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.
- e) El número de usuarios afectados.
- f) El volumen de facturación del responsable.
- g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
- h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

Artículo 39. *Proporcionalidad de sanciones.*

1. El órgano sancionador podrá establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

- a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 38.
- b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
- c) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán no acordar el inicio del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurren los siguientes presupuestos:

- a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en este real decreto-ley.
- b) Que el órgano competente no hubiese sancionado o apercibido al infractor en los dos años previos como consecuencia de la comisión de infracciones previstas en este real decreto-ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

3. No podrán ser objeto de apercibimiento las infracciones leves descritas en el artículo 36.4 c), d) y e) y la infracción grave prevista en el artículo 36.3 e).

Artículo 40. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 36 fuesen cometidas por órganos o entidades de las Administraciones Públicas, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al órgano o entidad infractora y a los afectados, si los hubiera.

Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.

2. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refiere el apartado anterior.

Artículo 41. *Competencia sancionadora.*

1. La imposición de sanciones corresponderá, en el caso de infracciones muy graves, al Ministro competente en virtud de lo dispuesto en el artículo 9, y en el caso de infracciones graves y leves al órgano de la autoridad competente que se determine mediante el reglamento de desarrollo de este real decreto-ley.

2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previstos en las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de

§ 9 Real Decreto-ley de seguridad de las redes y sistemas de información

las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones públicas. No obstante, el plazo máximo de duración del procedimiento será de un año y el plazo de alegaciones no tendrá una duración inferior a un mes.

Artículo 42. *Concurrencia de infracciones.*

1. No procederá la imposición de sanciones según lo previsto en este real decreto-ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

2. Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

Disposición adicional primera. *Relación inicial de servicios esenciales y operadores de servicios esenciales.*

La Comisión Nacional para la Protección de las Infraestructuras Críticas aprobará una primera lista de servicios esenciales dentro de los sectores incluidos en el ámbito de aplicación de este real decreto-ley e identificará a los operadores que los presten que deban sujetarse a este real decreto-ley en el siguiente orden:

a) Antes del 9 de noviembre de 2018: los servicios esenciales y los operadores correspondientes a los sectores estratégicos energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

b) Antes del 9 de noviembre de 2019: los servicios esenciales y los operadores correspondientes al resto de los sectores estratégicos recogidos en el anexo de la Ley 8/2011, de 28 de abril.

Disposición adicional segunda. *Comunicaciones electrónicas y servicios de confianza.*

La aplicación de este real decreto-ley a los operadores de redes y servicios de comunicaciones electrónicas y de servicios electrónicos de confianza que sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, no obstará a la aplicación de su normativa específica en materia de seguridad.

El Ministerio de Economía y Empresa, como órgano competente para la aplicación de dicha normativa, y el Ministerio del Interior actuarán de manera coordinada en el establecimiento de obligaciones que recaigan sobre los operadores críticos. Así mismo, mantendrán un intercambio fluido de información sobre incidentes que les afecten.

Disposición adicional tercera. *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley.*

La plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

Disposición adicional cuarta. *Proveedores de servicios digitales ya existentes.*

Los proveedores de servicios digitales que ya vinieran prestando servicios deberán comunicar su actividad a la Secretaría de Estado para el Avance Digital del Ministerio de Economía y Empresa, en el plazo de tres meses desde la entrada en vigor de este real decreto-ley.

Disposición final primera. *Título competencial.*

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.^a y 29.^a de la Constitución.

Disposición final segunda. *Incorporación del Derecho de la Unión Europea.*

Este real decreto-ley incorpora al ordenamiento jurídico interno la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Disposición final tercera. *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en este real decreto-ley sin perjuicio de la competencia de los Ministros para fijar las obligaciones específicas mediante Orden Ministerial en los supuestos previstos en el articulado de esta norma.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 10

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 24, de 28 de enero de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-1192

En el ámbito europeo, con el objetivo de dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información, se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems). Esta norma parte de un enfoque global de la seguridad de las redes y sistemas de información en la Unión Europea, integrando requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La transposición de la citada Directiva NIS al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

El Real Decreto-ley 12/2018, de 7 de septiembre, habilita al Gobierno, en su disposición final tercera, para su desarrollo reglamentario. Con esa cobertura legal, y en cumplimiento del citado mandato y lo previsto en sus artículos 9.1 a), 11.1 a), 11.2, 16.2, 16.3, 19.1 y 19.5, este real decreto tiene por finalidad desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.

El real decreto, en su artículo 3, pormenoriza la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información prevista en el artículo 9.1.a) 2.º del Real Decreto-ley 12/2018, de 7 de septiembre. Es oportuno mencionar, en relación con la seguridad en el sector de la alimentación, la participación de la Agencia Española de Seguridad Alimentaria y Nutrición, dependiente del Ministerio de Consumo. Adicionalmente,

y de conformidad con el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, el real decreto desarrolla los supuestos de cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia, y de estos con las autoridades competentes, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículo 4).

Con relación a la figura del punto de contacto único (artículo 5) que consagra la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se desarrollan sus funciones de enlace para garantizar la cooperación transfronteriza con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Por otra parte, el artículo 6 de este real decreto desarrolla las previsiones del artículo 16.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre las medidas necesarias para el cumplimiento de las obligaciones de seguridad por parte de los operadores de servicios esenciales, que habrán de concretarse en una declaración de aplicabilidad de medidas de seguridad suscrita por el responsable de seguridad de la información del operador, cuyas funciones también se desarrollan en el artículo 7 de este real decreto. El plazo para la designación del responsable de la seguridad se establece en cumplimiento de la habilitación recogida en el artículo 16.3 del Real Decreto-ley 12/2018, de 7 de septiembre.

Por lo que se refiere a la notificación de incidentes, el real decreto, en sus artículos 8 y 9, desarrolla las obligaciones de notificación por parte de los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales aun cuando no hayan tenido un efecto adverso real sobre aquellos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción nacional de notificación y gestión de ciberincidentes que se contiene en el anexo.

El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículos 10 y 11), a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información (artículos 12 a 14).

Por último, en materia de supervisión de requisitos de seguridad, el real decreto desarrolla en su artículo 15 la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir, asimismo, la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión.

En las disposiciones adicionales de este real decreto se recoge, entre otras materias, el régimen jurídico aplicable al Banco de España teniendo en cuenta su especial configuración jurídica como entidad de Derecho público con personalidad jurídica propia y plena capacidad pública y privada, que en el desarrollo de su actividad y para el cumplimiento de sus fines actúa con autonomía respecto a la Administración General del Estado, y como parte integrante del Sistema Europeo de Bancos Centrales (SEBC) y del Mecanismo Único de Supervisión (MUS). Esta especial configuración jurídica supone que el marco de seguridad de las redes y sistemas de información resulte de aplicación en la medida en que no interfiera con la naturaleza, funciones e independencia del Banco de España.

Este real decreto se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Responde, en primer lugar, a los principios de necesidad y eficacia, en tanto que la norma es necesaria para llevar a cabo el desarrollo reglamentario del Real Decreto-ley 12/2018, de 7 de septiembre, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 y, en concreto, para establecer el marco estratégico e institucional de seguridad de las redes y sistemas de información, las obligaciones de seguridad y la gestión de incidentes, siendo el instrumento más idóneo para la consecución de este objetivo. En segundo término, la norma cumple con el principio de proporcionalidad, al no existir otras medidas menos gravosas para los operadores de servicios esenciales y proveedores de servicios digitales destinadas a cumplir

la obligación de adoptar medidas técnicas y de organización para gestionar los riesgos para la seguridad de sus redes y sistemas de información, así como de notificar los incidentes que tengan efectos perturbadores significativos en los servicios que prestan. Asimismo, este real decreto cumple con el principio de seguridad jurídica, resultando el proyecto conforme a la directiva europea de la que trae causa, así como con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su normativa de desarrollo, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y la normativa comunitaria y nacional en materia de protección de datos. Se ha cumplido igualmente con el principio de transparencia, al haber sometido el proyecto de real decreto al trámite de audiencia, definiéndose claramente los objetivos de la iniciativa normativa y su justificación. Por último, este real decreto resulta conforme con el principio de eficiencia, dado que no se establecen cargas adicionales a las contempladas en el real decreto-ley que desarrolla.

En la elaboración de este real decreto se ha solicitado informe de todos los departamentos ministeriales, así como de la Agencia Española de Protección de Datos, de la Comisión Nacional de los Mercados y de la Competencia, de la Comisión Nacional del Mercado de Valores, del Consejo de Seguridad Nuclear, y del Banco de España. Adicionalmente, se ha solicitado informe a todas las comunidades autónomas y se ha dado audiencia a las organizaciones representativas de los sectores afectados.

En su virtud, a propuesta conjunta de la Vicepresidenta Tercera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, de la Ministra de Defensa, del Ministro del Interior y de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática, con la aprobación previa de la Ministra de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 26 de enero de 2021,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Este real decreto tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

Artículo 2. *Ámbito de aplicación.*

1. De conformidad con el artículo 2 del Real Decreto-ley 12/2018, de 7 de septiembre, este real decreto se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

De conformidad con lo previsto en el apartado 1 del artículo 6 del Real Decreto-ley 12/2018, la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo, en particular el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3. Este real decreto no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

4. De conformidad con el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en el Real Decreto-ley 12/2018, de 7 de septiembre, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

CAPÍTULO II

Marco estratégico e institucional

Artículo 3. *Autoridades competentes.*

Las autoridades competentes en materia de seguridad de las redes y sistemas de información serán, con carácter general, las establecidas en el artículo 9.1 del Real Decreto-ley 12/2018, de 7 de septiembre. En particular, son autoridades competentes para los operadores de servicios esenciales que no sean operadores críticos de acuerdo con la Ley 8/2011, de 28 de abril, y que no estén incluidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las siguientes:

a) Respecto al sector del transporte: el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.

b) Respecto al sector de la energía: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

c) Respecto al sector de las tecnologías de la información y las telecomunicaciones: el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

d) Respecto al sector del sistema financiero:

1.º El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones.

2.º El Banco de España, para las entidades de crédito.

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

3.º La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

e) Respecto al sector del espacio: el Ministerio de Defensa, a través de la Secretaría de Estado de Defensa.

f) Respecto al sector de la industria química: el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

g) Respecto al sector de las instalaciones de investigación: el Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación.

h) Respecto al sector de la salud: el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

i) Respecto al sector del agua: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.

j) Respecto al sector de la alimentación:

1.º El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación.

2.º El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

3.º El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.

4.º El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN).

k) Respecto al sector de la industria nuclear:

1.º El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

2.º El Consejo de Seguridad Nuclear.

Artículo 4. *Cooperación y coordinación de los CSIRT de referencia.*

1. La cooperación entre los CSIRT de referencia, y entre estos y las autoridades competentes, se instrumentará a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes regulada en el artículo 11.

2. A efectos de la cooperación prevista en el artículo 11.1.a) 3.º del Real Decreto-ley 12/2018, de 7 de septiembre, se entenderá que son operadores con incidencia en la Defensa Nacional aquellos proveedores de servicios esenciales básicos para el funcionamiento del Ministerio de Defensa o para la operatividad de las Fuerzas Armadas que se establezcan, a propuesta del Ministerio de Defensa, por la Comisión Nacional para la Protección de las Infraestructuras Críticas.

La designación como operador con incidencia en la Defensa Nacional se llevará a cabo de conformidad con lo previsto en el Reglamento de protección de las infraestructuras críticas, aprobado por el Real Decreto 704/2011, de 20 de mayo. Así mismo, los CSIRT de referencia serán informados de la identidad de los operadores de servicios esenciales de su comunidad que sean designados operadores con incidencia en la Defensa Nacional.

El Ministerio de Defensa comunicará oportunamente a la Comisión Nacional para la Protección de las Infraestructuras Críticas las actualizaciones derivadas de cambios de operadores en la provisión de estos servicios, que activarán las correspondientes notificaciones de alta o baja como operadores con incidencia en la Defensa Nacional tanto a los propios operadores como a sus CSIRT de referencia.

Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, este pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas. En el caso de que así fuera, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará al ESPDEF-CERT del Mando Conjunto del Ciberespacio a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente.

3. Los supuestos de especial gravedad a los que se refiere el artículo 11.2 párrafo primero del Real Decreto-ley 12/2018, de 7 de septiembre, en los que el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT, serán todos aquellos que,

atendiendo a la naturaleza de las notificaciones inicial o sucesivas del incidente recibidas por el CSIRT de referencia, posean un impacto o nivel de peligrosidad muy alta o crítica de acuerdo con lo establecido en el anexo, y exijan un nivel de coordinación técnica con los otros CSIRT de referencia superior al necesario en situaciones ordinarias.

El Consejo Nacional de Ciberseguridad será inmediatamente informado y podrá desactivar la coordinación prevista en este artículo, que únicamente podrá producirse cuando haya cesado la situación prevista en el párrafo anterior y que no afectará al proceso de notificación de incidentes regulados en los artículos 11, 19.1 y 19.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. El CCN-CERT, en el caso previsto en el apartado anterior, y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior (OCC), en los supuestos previstos en el artículo 11.2 párrafo segundo del Real Decreto-ley 12/2018, de 7 de septiembre, requerirán al CSIRT de referencia, tras la primera notificación del incidente, al menos la siguiente información:

a) Confirmación de que son correctos los datos asignados al incidente, en particular verificando, si existe esta información, la validez de:

- 1.º La clasificación del incidente.
- 2.º La peligrosidad del incidente.
- 3.º El impacto del incidente.

b) Plan de acción del CSIRT para abordar la resolución técnica del incidente, si procede.

c) Cualquier información que permita determinar el posible impacto transfronterizo del incidente.

Siempre que sea posible se empleará la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes para las comunicaciones consideradas en este apartado.

Artículo 5. Punto de contacto único.

1. En su función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9 del Real Decreto-ley 12/2018, de 7 de septiembre, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación contemplado en el artículo 11 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, y la red de CSIRT, el Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional:

a) Comunicará a la Comisión Europea la lista de los operadores de servicios esenciales nacionales establecidos para cada sector y subsector a los que se refiere el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre e informará a los puntos de contacto único de otros Estados sobre la intención de identificación de un operador de servicios esenciales de otro Estado miembro que ofrezca servicios en España.

b) Transmitirá a los puntos de contacto de otros Estados miembros de la Unión Europea afectados la información sobre incidentes con impacto transfronterizo que le transmitan las autoridades competentes o CSIRT de referencia, según lo establecido en el artículo 25 del Real Decreto-ley 12/2018, de 7 de septiembre.

c) Remitirá a los CSIRT de referencia y a las autoridades competentes nacionales la correspondiente información sobre incidentes que puedan tener efectos perturbadores en los servicios esenciales que reciba de los puntos de contacto de los correspondientes Estados miembros, para que adopten las medidas oportunas en el ejercicio de sus funciones respectivas.

d) Dictará las instrucciones pertinentes a las autoridades competentes para que elaboren, anualmente, el informe al que se refiere el artículo 27.1 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre el tipo y número de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea, teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

e) Recabará de las autoridades competentes el informe anual al que se refiere la letra anterior, y elaborará un informe anual resumido sobre las notificaciones recibidas, que

remitirá al grupo de cooperación antes del 15 de febrero de cada año y, posteriormente, a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

2. Adicionalmente a las funciones de enlace previstas en el apartado anterior, y de conformidad con lo previsto en el artículo 9.2 del Real Decreto-ley 12/2018, de 7 de septiembre, el Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, garantizará la coordinación de las actuaciones de las autoridades competentes mediante:

a) El fomento de la coherencia entre los requisitos de seguridad específicos que en su caso adopten las autoridades competentes, conforme a lo previsto en el artículo 6.6 de este real decreto.

b) El fomento de la coherencia entre las obligaciones específicas que en su caso establezcan las autoridades competentes, conforme a lo previsto en el artículo 8.3 de este real decreto.

c) El impulso de la coordinación de las disposiciones y actuaciones de las autoridades competentes y las actuaciones de los CSIRT de referencia con las disposiciones y actuaciones en materia de seguridad de la información de las autoridades de protección de datos y de seguridad pública.

3. Del mismo modo, el Consejo de Seguridad Nacional ejercerá las funciones de coordinación previstas en el apartado 2 anterior en los supuestos contemplados en el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre.

CAPÍTULO III

Requisitos de seguridad

Artículo 6. *Medidas para el cumplimiento de las obligaciones de seguridad.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y sistemas propios, como de proveedores externos.

2. En el caso de los operadores de servicios esenciales, deberán aprobar unas políticas de seguridad de las redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

Dichas políticas considerarán, como mínimo, los siguientes aspectos:

- a) Análisis y gestión de riesgos.
- b) Gestión de riesgos de terceros o proveedores.
- c) Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.
- d) Gestión del personal y profesionalidad.
- e) Adquisición de productos o servicios de seguridad.
- f) Detección y gestión de incidentes.
- g) Planes de recuperación y aseguramiento de la continuidad de las operaciones.
- h) Mejora continua.
- i) Interconexión de sistemas.
- j) Registro de la actividad de los usuarios.

3. Las medidas de seguridad que se adopten por los operadores de servicios esenciales deberán tener en cuenta, en particular, la dependencia de las redes y sistemas de información y la continuidad de servicios o suministros contratados por el operador, así como las interacciones que presenten con redes y sistemas de información de terceros.

4. La relación de medidas adoptadas se formalizará en un documento denominado Declaración de Aplicabilidad de medidas de seguridad, que será suscrito por el responsable de seguridad de la información designado conforme a lo previsto en el artículo siguiente y que se incluirá en la política de seguridad que apruebe la Dirección de la organización. Dicho documento, que deberá remitirse a la autoridad competente respectiva en el plazo de seis

meses desde la designación del operador como operador de servicios esenciales, deberá revisarse, al menos, cada tres años. Tanto la Declaración de Aplicabilidad de medidas de seguridad inicial, como sus sucesivas revisiones serán objeto de supervisión por la autoridad competente respectiva, según se prevé en el artículo 14 de este real decreto.

5. Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes.

Sin perjuicio de lo anterior, podrán tenerse en cuenta otros estándares reconocidos internacionalmente.

6. Las medidas adoptadas podrán ser complementadas con otras, atendiendo a necesidades específicas, entre ellas, la posibilidad de exigir un documento de aplicabilidad de los sistemas afectados por esta normativa, en aquellos operadores con entornos de sistemas de información especialmente complejos. En particular, se complementarán con las que, en su caso, establezcan con carácter específico las autoridades competentes, de conformidad con lo previsto en el artículo 16.4 y el artículo 32.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

7. En la elaboración de las políticas de seguridad de las redes y sistemas de información se tendrán en cuenta los riesgos que se derivan del tratamiento de los datos personales, de acuerdo con el artículo 24 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de protección de datos). En caso de que el análisis de gestión de riesgos de acuerdo con el Reglamento general de protección de datos exija medidas adicionales a implantar respecto de las previstas en el Real Decreto 3/2010, de 8 de enero, se adoptarán las medidas de acuerdo con el artículo 24.1 del Reglamento general de protección de datos.

Artículo 7. Responsable de la seguridad de la información.

1. Los operadores de servicios esenciales designarán una persona, unidad u órgano colegiado, responsable de la seguridad de la información que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y CSIRT de referencia que le corresponda de conformidad con lo previsto en el apartado tercero. En el supuesto de que el responsable de seguridad de la información sea una unidad u órgano colegiado, se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad. El plazo para llevar a cabo dicha designación será de tres meses desde su designación como operador de servicios esenciales.

2. Los operadores de servicios esenciales comunicarán a la autoridad competente respectiva la designación del responsable de la seguridad de la información dentro del plazo establecido en el apartado anterior, así como los nombramientos y ceses que afecten a la designación del responsable de la seguridad de la información en el plazo de un mes desde que aquellos se produzcan.

3. El responsable de la seguridad de la información actuará como punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información, y como punto de contacto especializado para la coordinación de la gestión de los incidentes con el CSIRT de referencia. Se desarrollarán bajo su responsabilidad, entre otras, las siguientes funciones:

a) Elaborar y proponer para aprobación por la organización, de conformidad con lo establecido en el artículo 6.2 de este real decreto, las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios, de conformidad con lo dispuesto en el artículo 6.

b) Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

c) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.3 párrafo segundo de este real decreto.

d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

e) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

f) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

g) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

El responsable de la seguridad de la información, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

4. Los operadores de servicios esenciales garantizarán que el responsable de la seguridad de la información cumpla con los siguientes requisitos:

a) Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de las funciones indicadas en el apartado anterior.

b) Contar con los recursos necesarios para el desarrollo de dichas funciones.

c) Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.

d) Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

5. Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, las funciones y responsabilidades encomendadas al responsable de la seguridad de la información podrán compatibilizarse con las señaladas para el Responsable de Seguridad y Enlace y el Responsable de Seguridad del Esquema Nacional de Seguridad, de conformidad con lo dispuesto en la normativa aplicable a estas figuras.

CAPÍTULO IV

Gestión de incidentes de seguridad

Artículo 8. *Gestión de incidentes de seguridad.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. En el caso de redes y sistemas que no sean propios los operadores deberán tomar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos.

Esta obligación alcanza tanto a los incidentes detectados por el propio operador o proveedor como a los que les señalen el CSIRT de referencia o la autoridad competente, cuando tengan conocimiento de alguna circunstancia que haga sospechar de la existencia de un incidente.

2. Sin perjuicio de lo previsto en el artículo 28.1 del Real Decreto-ley 12/2018, de 7 de septiembre, los operadores de servicios esenciales y los proveedores de servicios digitales podrán solicitar voluntariamente ayuda especializada del CSIRT de referencia para la gestión de los incidentes, debiendo en tales casos atender a las indicaciones que reciban de este para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

3. En la resolución de los incidentes, los operadores de servicios esenciales aplicarán los aspectos pertinentes de la política de gestión de la seguridad de las redes y sistemas de

información a la que se refiere el artículo 6, así como las obligaciones específicas que en su caso establezcan las autoridades competentes.

Artículo 9. *Obligaciones de notificación de incidentes de los operadores de servicios esenciales.*

1. Los operadores de servicios esenciales notificarán a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto, según el detalle que se especifica en el apartado 4 de la Instrucción nacional de notificación y gestión de ciberincidentes, que se contiene en el anexo de este real decreto.

Asimismo, notificarán los sucesos o incidencias que, por su nivel de peligrosidad, puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido todavía un efecto adverso real sobre aquellos. A estos efectos, se considerarán los incidentes con un nivel de peligrosidad crítico, muy alto o alto, según el detalle que se especifica en el apartado 3 de la citada Instrucción.

2. Sin perjuicio de lo anterior, las autoridades competentes podrán establecer, de conformidad con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre, obligaciones específicas de notificación que contemplen niveles diferentes a los previstos en la Instrucción nacional de notificación y gestión de ciberincidentes, así como factores y umbrales sectoriales específicos, aplicables a los operadores sometidos a su supervisión.

3. La notificación de un ciberincidente conforme a este real decreto no excluye ni sustituye la notificación que de los mismos hechos deba realizarse a otros organismos conforme a su normativa específica.

En particular, las obligaciones de notificación previstas en los apartados anteriores son independientes de las que deban realizarse a la Agencia Española de Protección de Datos conforme a lo previsto en el artículo 33 del Reglamento general de protección de datos, sin perjuicio de la cooperación entre autoridades prevista en el artículo 29 del Real Decreto-ley 12/2018, y la posibilidad de acceso por parte de la citada agencia a la plataforma común de notificación de incidentes prevista en su disposición adicional tercera.

A estos efectos, las notificaciones previstas en los apartados 1 y 2 de este artículo incluirán la información que, para los casos de violación de la seguridad de los datos personales, se contenga en los formularios aprobados por la Agencia Española de Protección de Datos.

Artículo 10. *Procedimientos de notificación de incidentes.*

1. Los CSIRT de referencia garantizarán un intercambio fluido de información con las autoridades competentes que correspondan, asegurando el adecuado seguimiento durante la gestión de los incidentes, así como el acceso a la información empleada en las distintas fases que componen la gestión de incidentes.

2. Los operadores de servicios esenciales realizarán las notificaciones a través del responsable de la seguridad de la información designado.

En el caso de que un operador de servicios esenciales reúna los criterios previstos en el artículo 6.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información, el responsable de la seguridad de la información se coordinará a estos efectos con el Responsable de Seguridad y Enlace previsto en el artículo 16 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

3. Los operadores de servicios esenciales deberán realizar una primera notificación tan pronto como dispongan de información para determinar que se dan las circunstancias para la notificación, atendiendo a los factores y umbrales correspondientes.

Se efectuarán las notificaciones intermedias que sean precisas para actualizar o completar la información incorporada a la notificación inicial, e informar sobre la evolución del incidente, mientras este no esté resuelto, y se realizará una notificación final del incidente tras su resolución, informando del detalle de la evolución del suceso, la valoración de la probabilidad de su repetición, y las medidas correctoras que eventualmente tenga previsto

adoptar el operador. Los umbrales temporales exigidos para dichas notificaciones serán los recogidos en el anexo de este real decreto.

4. Las notificaciones incluirán, en cuanto esté disponible, la información que permita determinar cualquier efecto transfronterizo del incidente.

5. Lo establecido en los apartados anteriores será de aplicación a los proveedores de servicios digitales en tanto que no se regule de modo diferente en los actos de ejecución previstos en el artículo 16.9 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

6. El CSIRT de referencia, en colaboración con la autoridad competente, valorará con prontitud dicha información con vistas a determinar si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en otros Estados miembros de la Unión Europea, informando en tal caso a través del punto de contacto único a los Estados miembros afectados.

Asimismo, la autoridad competente valorará, conjuntamente con el correspondiente CSIRT de referencia, la información sobre incidentes con posibles impactos transfronterizos que reciba de otros Estados miembros, y se lo indicará y transmitirá la información relevante a los operadores de servicios esenciales que puedan verse afectados.

Artículo 11. *Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.*

1. El CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT del Mando Conjunto del Ciberespacio pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes a la que se refiere el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre.

2. La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.

3. Esta plataforma deberá garantizar asimismo la disponibilidad, autenticidad, integridad y confidencialidad de la información, así como podrá emplearse también para dar cumplimiento a la exigencia de notificación derivada de regulaciones sectoriales, de acuerdo con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. La plataforma dispondrá asimismo de diversos canales de comunicación para su uso por parte de las autoridades competentes y los CSIRT de referencia. La plataforma garantizará el acceso de las autoridades competentes a toda la información relativa a la notificación y estado de situación de los incidentes de su ámbito de competencia que les permita efectuar en todo momento el necesario seguimiento y control de su estado de situación. Igualmente, las autoridades competentes tendrán acceso a través de la plataforma a datos estadísticos, en particular a los necesarios para generar los informes a los que hace mención el artículo 5.

5. Asimismo, la plataforma implementará el procedimiento de notificación y gestión de incidentes, que estará disponible durante todas las horas del día y todos los días del año, y dispondrá como mínimo de las siguientes capacidades:

- a) Capacidad de gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros, según lo establecido en el anexo.
- b) Capacidad de intercambio de información sobre ciberamenazas.
- c) Capacidad de análisis de muestras.
- d) Capacidad de registro y notificación de vulnerabilidades.
- e) Capacidad de comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.
- f) Capacidad de intercambio masivo de datos.
- g) Generación de estadísticas e informes agregados.

Artículo 12. *Información sobre incidentes.*

1. Cuando las circunstancias lo permitan, los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales notificantes la información pertinente con respecto al seguimiento de la notificación de un incidente, en particular aquella que pueda facilitar la gestión eficaz del incidente.

2. Asimismo, las autoridades competentes y los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales que pudieran verse afectados por dichos incidentes la información que pudiera serles relevante para prevenir y en su caso resolver el incidente.

3. Al proporcionar la información a la que se refieren los apartados anteriores, las autoridades competentes y los CSIRT de referencia velarán por los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, preservando la confidencialidad de la información que recaben de estos, de conformidad con lo establecido en el artículo 15 del Real Decreto-ley 12/2018, de 7 de septiembre.

Artículo 13. *Actuaciones ante incidentes con carácter presuntamente delictivo.*

En cumplimiento de lo dispuesto en el artículo 262 de la Ley de Enjuiciamiento Criminal, la OCC comunicará a la mayor brevedad posible al Ministerio Fiscal y, en su caso, a las Unidades orgánicas de Policía Judicial competentes, aquellos incidentes de seguridad que le sean notificados y que revistan carácter presuntamente delictivo, trasladando al tiempo la información que posea en relación con ello. A dicho fin podrá requerir de los operadores afectados o de los CSIRT de referencia cuanta información relacionada con el incidente se estime necesaria.

Artículo 14. *Consulta con otras autoridades.*

1. Las consultas con otras autoridades con competencia en materia de seguridad pública y seguridad ciudadana, previstas en el artículo 14.1 del Real Decreto-ley 12/2018, de 7 de septiembre, se realizarán a través de la OCC.

2. Las consultas relativas al resto de materias previstas en el citado artículo 14 se realizarán directamente a las autoridades competentes correspondientes.

CAPÍTULO V

Supervisión

Artículo 15. *Supervisión del cumplimiento de obligaciones de seguridad y de notificación de incidentes.*

1. Las autoridades competentes supervisarán en su ámbito de actuación el cumplimiento de las obligaciones de seguridad y de notificación de incidentes que sean de aplicación a los operadores de servicios esenciales y a los proveedores de servicios digitales de conformidad con el Real Decreto-ley 12/2018, de 7 de septiembre, y este real decreto.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales colaborarán con la autoridad competente en dicha supervisión, facilitando las actuaciones de inspección, proporcionando toda la información que a tal efecto se les requiera, y aplicando las instrucciones dictadas, en su caso, para la subsanación de las deficiencias observadas.

3. El cumplimiento de las obligaciones de seguridad en las redes y sistemas de información podrá ser acreditado mediante la certificación en un esquema de seguridad que, previa consulta al CSIRT de referencia, sea reconocido por la autoridad competente.

4. Las autoridades competentes podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control. En particular, las actuaciones de inspección de las autoridades competentes, que podrán ser apoyadas por los CSIRT de referencia, tendrán por objeto:

a) Controlar el cumplimiento de las normas e instrucciones técnicas que, en su caso, resulten aplicables a los operadores sujetos a su supervisión.

b) Verificar el cumplimiento de las funciones del responsable de seguridad de la información designado por los operadores de servicios esenciales, según lo previsto en el artículo 7.3 de este real decreto.

c) Realizar las comprobaciones, inspecciones, pruebas y revisiones necesarias para verificar el cumplimiento de las medidas de seguridad previstas en el artículo 6, en particular, la política de seguridad de los operadores de servicios esenciales y la Declaración de aplicabilidad de medidas de seguridad.

De conformidad con lo previsto en el artículo 32.1 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando el volumen o complejidad de las actuaciones de inspección que deban desarrollarse así lo aconseje, las autoridades competentes podrán requerir al operador de servicios esenciales la remisión de un informe de auditoría, elaborado por una entidad externa, solvente e independiente, sobre la seguridad de sus redes y sistemas de información.

5. Los CSIRT de referencia colaborarán con las autoridades competentes, cuando estas se lo requieran, en el ejercicio de las funciones a las que se refiere el apartado anterior. En particular, facilitarán asesoramiento técnico sobre la idoneidad de las medidas de seguridad adoptadas por los operadores de servicios esenciales y los proveedores de servicios digitales en virtud del artículo 6 de este real decreto.

Asimismo, cuando se trate de operadores con incidencia en la Defensa Nacional a que se refiere el artículo 4.2 de este real decreto, el ESPDEF-CERT del Mando Conjunto del Ciberespacio podrá colaborar en la supervisión con la autoridad competente.

6. En el caso de los proveedores de servicios digitales la supervisión se llevará a cabo de manera coordinada con las autoridades competentes correspondientes de los Estados miembros de la Unión Europea donde dichos proveedores presten servicios o tengan su establecimiento principal en la Unión.

Disposición adicional primera. *Designación del responsable de la seguridad de la información por los operadores de servicios esenciales designados.*

Los operadores de servicios esenciales designados conforme a lo previsto en la disposición adicional primera del Real Decreto-ley 12/2018, de 7 de septiembre, deberán comunicar a la autoridad competente respectiva la identidad del responsable de la seguridad de la información en el plazo de tres meses desde la entrada en vigor de este real decreto.

Disposición adicional segunda. *Orientaciones para la gestión de incidentes y cumplimiento de las obligaciones de notificación.*

El Consejo de Seguridad Nacional, a propuesta de su comité especializado en materia de ciberseguridad, y articuladas sus funciones como punto de contacto único a través del Departamento de Seguridad Nacional, podrá aprobar orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes recogida en el anexo, así como para la actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes, que incluyan directrices y recomendaciones para el cumplimiento de las obligaciones de notificación previstas en este real decreto, así como en el Real Decreto-ley 12/2018, de 7 de septiembre, con objeto de mejorar la coordinación y optimizar los recursos dedicados a la gestión de los incidentes que afecten a la seguridad de las redes y sistemas de información.

Disposición adicional tercera. *Régimen específico del Banco de España.*

Las disposiciones del presente real decreto se entenderán sin perjuicio de las competencias y funciones atribuidas al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, de conformidad con el Tratado de Funcionamiento de la Unión Europea, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo, Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito, y la Ley 13/1994, de 1 de junio, de Autonomía del Banco de España.

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

En lo no previsto en su normativa específica, y en cuanto sea compatible con su naturaleza, funciones e independencia, será de aplicación al Banco de España lo previsto en este real decreto.

Disposición adicional cuarta. *Supuesto de dependencia de proveedores externos.*

En referencia al artículo 19.3 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando los operadores de servicios esenciales o proveedores de servicios digitales dependan de proveedores externos a los que les sea de aplicación la disposición adicional novena de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, el Equipo de Respuesta ante Emergencias Informáticas (CERT) competente del proveedor externo se corresponderá con:

- a) El CCN-CERT, del Centro Criptológico Nacional, cuando el proveedor esté incluido en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.
- b) El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, en el resto de los casos.

Disposición adicional quinta. *Tratamientos de datos de carácter personal.*

Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a su libre circulación; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, en su caso, en la normativa sobre protección de datos personales especial o específica que resulte de aplicación.

Disposición adicional sexta. *Información sobre incidentes en el sistema financiero.*

Los CSIRT de referencia informarán al titular de la Secretaría de Estado de Economía y Apoyo a la Empresa, a través de la Secretaría General del Tesoro y Financiación Internacional, de los incidentes que puedan tener efectos perturbadores significativos en los servicios esenciales del sistema financiero. A estos efectos, se entenderá que tienen efectos perturbadores significativos cuando su umbral o nivel de impacto sea crítico, muy alto o alto, según lo señalado en el anexo de este real decreto.

Disposición transitoria única. *Desempeño transitorio de funciones en el sector energético.*

La Secretaría de Estado de Seguridad del Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad (OCC), desempeñará temporalmente las funciones atribuidas por este real decreto al departamento ministerial con competencias en materia de energía, hasta que este disponga de los recursos humanos necesarios con la formación adecuada para ejercer estas competencias de forma efectiva según lo previsto en el artículo 3 y, en todo caso, en un plazo máximo de 12 meses.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de lo previsto en el artículo 149.1.21.^a y 29.^a de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de telecomunicaciones y seguridad pública, respectivamente.

Disposición final segunda. *Habilitación para el desarrollo normativo y aplicación.*

Se faculta a los titulares de los Ministerios de Asuntos Económicos y Transformación Digital, Interior y Defensa, así como a los titulares de los Ministerios y organismos relacionados en el artículo 3, para dictar conjunta o separadamente, según las materias de que se trate, y en el ámbito de sus respectivas competencias, las disposiciones que exijan el desarrollo y aplicación de este real decreto.

Disposición final tercera. Entrada en vigor.

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Instrucción nacional de notificación y gestión de ciberincidentes

1. Obligatoriedad de notificación

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en esta instrucción, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel CRÍTICO, MUY ALTO o ALTO para todos aquellos sujetos obligados a los que les sea aplicable esta «Instrucción nacional de notificación y gestión de ciberincidentes». En ese caso, los sujetos obligados deberán comunicar, en tiempo y forma, los incidentes que registren en sus redes y sistemas de información y que estén obligados a notificar por superar los umbrales de impacto o peligrosidad establecidos en esta instrucción.

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el nivel de peligrosidad que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado nivel de impacto que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente debido a sus características potenciales, este se asociará a aquel que tenga un nivel de peligrosidad superior de acuerdo a los criterios expuestos en esta Instrucción.

2. Clasificación/taxonomía de los ciberincidentes

La siguiente Clasificación/Taxonomía de los ciberincidentes está alineada con la taxonomía aprobada por la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Esta Clasificación/Taxonomía de los ciberincidentes se empleará para la asignación de una clasificación específica a un incidente registrado en las redes y sistemas de información cuando se realice la comunicación a la autoridad competente o CSIRT de referencia.

Tabla 1. Clasificación/Taxonomía de los ciberincidentes

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Contenido abusivo.	Spam.	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delitos de odio, contra la libertad o el honor.	Contenido difamatorio o discriminatorio. Ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado.	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino.	Sistema infectado.	Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un <i>rootkit</i> .
	Servidor C&C (Mando y Control).	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware.	Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.
Obtención de información.	Configuración de malware.	Recurso que aloje ficheros de configuración de malware Ej.: ataque de <i>webinjects</i> para trojano.
	Escaneo de redes (<i>scanning</i>).	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeos para recopilar información de alojamientos, servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (<i>sniffing</i>).	Observación y grabación del tráfico de redes.
Intento de intrusión.	Ingeniería social.	Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.
	Explotación de vulnerabilidades conocidas.	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de <i>buffer</i> , puertas traseras, <i>cross site scripting</i> (XSS).
	Intento de acceso con vulneración de credenciales.	Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.
Intrusión.	Ataque desconocido.	Ataque empleando <i>exploit</i> desconocido.
	Compromiso de cuenta con privilegios.	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios.	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones.	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.
	Robo.	Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

Clasificación	Tipo de incidente	Descripción y ejemplos prácticos
Disponibilidad.	DoS (Denegación de servicio).	Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación <i>web</i> que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio).	Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración.	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje.	Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.
	Interrupciones.	Interrupciones por causas ajenas. Ej.: desastre natural.
Compromiso de la información.	Acceso no autorizado a información.	Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información.	Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante <i>ransomware</i> .
	Pérdida de datos.	Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.
Fraude.	Uso no autorizado de recursos.	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor.	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: <i>Warez</i> .
	Suplantación.	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
	<i>Phishing</i> .	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerabilidad.	Criptografía débil.	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej.: servidores <i>web</i> susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS.	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej.: DNS <i>open-resolvers</i> o Servidores NTP con monitorización <i>monlist</i> .
	Servicios con acceso potencial no deseado.	Ej.: Telnet, RDP o VNC.
	Revelación de información.	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej.: SNMP o Redis.
	Sistema vulnerable.	Sistema vulnerable. Ej.: mala configuración de <i>proxy</i> en cliente (WPAD), versiones desfasadas de sistema.
Otros.	Otros.	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT.	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

3. Nivel de peligrosidad del ciberincidente

El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel crítico:

- APT.

Nivel muy alto:

- Distribución de malware.
- Configuración de malware.
- Robo.
- Sabotaje.
- Interrupciones.

Nivel alto:

- Pornografía infantil, contenido sexual o violento inadecuado.
- Sistema infectado.
- Servidor C&C (Mando y Control).
- Compromiso de aplicaciones.
- Compromiso de cuentas con privilegios.
- Ataque desconocido.
- DoS (Denegación de servicio).
- DDoS (Denegación distribuida de servicio).
- Acceso no autorizado a información.
- Modificación no autorizada de información.
- Pérdida de datos.
- *Phishing*.

Nivel medio:

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

- Discurso de odio.
- Ingeniería social.
- Explotación de vulnerabilidades conocidas.
- Intento de acceso con vulneración de credenciales.
- Compromiso de cuentas sin privilegios.
- Desconfiguración.
- Uso no autorizado de recursos.
- Derechos de autor.
- Suplantación.
- Criptografía débil.
- Amplificador DDoS.
- Servicios con acceso potencial no deseado.
- Revelación de información.
- Sistema vulnerable.

Nivel bajo:

- *Spam*.
- Escaneo de redes (*scanning*).
- Análisis de paquetes (*sniffing*).
- Otros.

4. Nivel de impacto del ciberincidente

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que tal ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo a ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares).

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:

- Impacto en la Seguridad Nacional o en la seguridad ciudadana.
- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO, SIN IMPACTO.

Nivel crítico:

- Afecta apreciablemente a la Seguridad Nacional.
- Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
- Afecta a una infraestructura crítica.
- Afecta a sistemas clasificados SECRETO.
- Afecta a más del 90 % de los sistemas de la organización.
- Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.
- El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
- Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.
- Extensión geográfica supranacional.
- Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

Nivel muy alto:

- Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
- Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
- Afecta a un servicio esencial.
- Afecta a sistemas clasificados RESERVADO.
- Afecta a más del 75 % de los sistemas de la organización.
- Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.
- El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
- Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.
- Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias).
- Daños reputacionales a la imagen del país (marca España).
- Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel alto:

- Afecta a más del 50 % de los sistemas de la organización.
- Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.
- El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.
- Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.
- Extensión geográfica superior a 3 CC.AA.
- Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

Nivel medio:

- Afecta a más del 20 % de los sistemas de la organización.
- Interrupción en la prestación del servicio superior al 5 % de usuarios.
- El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
- Impacto económico entre el 0,001 % y el 0,03 % del PIB actual.
- Extensión geográfica superior a 2 CC.AA.
- Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

Nivel bajo:

- Afecta a los sistemas de la organización.
- Interrupción de la prestación de un servicio.
- El ciberincidente precisa para resolverse menos de 1 Jornada-Persona.
- Impacto económico entre el 0,0001 % y el 0,001 % del PIB actual.
- Extensión geográfica superior a 1 CC.AA.
- Daños reputacionales puntuales, sin eco mediático.

Sin impacto:

- No hay ningún impacto apreciable.

5. Información a notificar a la autoridad competente en caso de incidente

El sujeto obligado comunicará, en la notificación inicial, todos aquellos campos acerca de los que tenga conocimiento en ese momento de acuerdo a la siguiente tabla, siendo posteriormente preceptiva la cumplimentación de todos los campos de la tabla en la notificación final del incidente.

Tabla 2. Información a notificar a la autoridad competente en caso de incidente

Qué notificar	Descripción
Asunto.	Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
OSE/PSD.	Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.
Sector estratégico.	Energía, transporte, financiero, etc.
Fecha y hora del incidente.	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección del incidente.	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.
Descripción.	Describir con detalle lo sucedido.
Recursos tecnológicos afectados.	Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones....
Origen del incidente.	Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.
Taxonomía (clasificación).	Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.
Nivel de peligrosidad.	Especificar el nivel de peligrosidad asignado a la amenaza.
Nivel de impacto.	Especificar el nivel de impacto asignado al incidente.
Impacto transfronterizo.	Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea.
Plan de acción y contramedidas.	Actuaciones realizadas hasta el momento en relación al ciberincidente. Indicar el Plan de acción seguido junto con las contramedidas implantadas.
Afectación.	Indicar si el afectado es una empresa o un particular, y las afectaciones según el nivel de impacto asignado.
Medios necesarios para la resolución (J-P).	Capacidad empleada en la resolución del incidente en Jornadas-Persona.
Impacto económico estimado (Si se conoce).	Costes asociados al incidente, tanto de carácter directo como indirecto.
Extensión geográfica (Si se conoce).	Local, autonómico, nacional, supranacional, etc.
Daños reputacionales (Si se conocen).	Afectación a la imagen corporativa del operador.
Adjuntos.	Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).
Regulación afectada.	ENS / RGPD / NIS / PIC / Otros.
Se requiere actuación de FCCSE.	Si / No.

6. Ventana temporal de reporte

Todos aquellos sujetos obligados que se vean afectados por un incidente de obligada notificación a la autoridad competente, a través del CSIRT de referencia, remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo a la siguiente ventana temporal de reporte.

- La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.
- La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.
- La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

No obstante lo anterior, se aportarán todas aquellas notificaciones adicionales intermedias o posteriores que se consideren necesarias.

Tabla 3. Ventana temporal de reporte

Nivel de peligrosidad o impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO.	Inmediata.	24/48 horas.	20 días.
MUY ALTO.	Inmediata.	72 horas.	40 días.
ALTO.	Inmediata.	–	–
MEDIO.	–	–	–
BAJO.	–	–	–

Los tiempos reflejados en la tabla 3 para la «notificación intermedia» y la «notificación final» tienen como referencia el momento de remisión de la «notificación inicial». La «notificación inicial» tiene como referencia de tiempo el momento de tener conocimiento del incidente.

7. Definiciones y conceptos

La descripción de las conductas aquí incluidas tiene carácter técnico y se entiende a los meros efectos de la notificación y gestión de ciberincidentes. Como tal, es independiente tanto de la calificación de los hechos, como de la aplicación por parte de la autoridad judicial

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

de los tipos penales establecidos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Contenido abusivo:

– Correo masivo no solicitado (*spam*): correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

– Acoso: referido a acoso virtual o ciberacoso, se trata del uso de medios de comunicación digitales para acosar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada o íntima, o falsa.

– Extorsión: obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a esta, o bien con ánimo de lucro de la que lo provoca.

– Mensajes ofensivos: comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

– Delito: cualquier acción tipificada como delito de acuerdo a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

– Pederastia: cualquier comportamiento relacionado con los descritos en el título VIII la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relativos a la captación o utilización de menores de edad o personas con discapacidad necesitadas de especial protección en actos que atenten contra su indemnidad o libertad sexual.

– Racismo: cualquier infracción penal, incluyendo infracciones contra las personas o las propiedades, donde la víctima, el local o el objetivo de la infracción se elija por su real o percibida, conexión, simpatía, filiación, apoyo o pertenencia a un grupo social, raza, religión o condición sexual.

– Apología de la violencia: exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.

Contenido dañino:

– *Malware* (código dañino): palabra que deriva de los términos *malicious* y *software*. Cualquier pieza de *software* que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como *malware*. Así pues *malware* es un término que engloba varios tipos de programas dañinos.

– Virus: tipo de *malware* cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos en correos electrónicos. No obstante también puede hacerlo a través de *scripts*, documentos, y vulnerabilidades XSS presentes en la *web*. Es reseñable que un virus requiere la acción humana para su propagación a diferencia de otro *malware*, véase Gusano.

– Gusano: programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

– Troyano: tipo de *malware* que se enmascara como *software* legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el *software* dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de *software*.

– Programa espía (*spyware*): tipo de *malware* que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir *keyloggers*,

monitorizaciones, recolección de datos así como robo de datos. Los *spyware* se pueden difundir como un troyano o mediante explotación de *software*.

– *Rootkit*: conjunto de *software* dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por máquina se entiende todo el espectro de sistemas IT, desde *smartphones* hasta ICS. El propósito por tanto de un *rootkit* es enmascarar eficazmente *payloads* y permitir su existencia en el sistema.

– *Dialer*: tipología de *malware* que se instala en una máquina y, de forma automática y sin consentimiento del usuario, realiza marcaciones telefónicas a número de tarificación especial. Estas acciones conllevan costes económicos en la víctima al repercutir el importe de la comunicación.

– *Ransomware*: se engloba bajo este epígrafe a aquel *malware* que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

– *Bot* dañino: una *botnet* es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un *bot* es una pieza de *software* maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los *bots* y que ejecuten las órdenes dictadas remotamente.

– RAT: del inglés *Remote Access Tool*, se trata de una funcionalidad específica de control remoto de un sistema de información, que incorporan determinadas familias o muestras de *software* dañino (*malware*).

– C&C: del inglés *Command and Control*, se refiere a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos *zombie* infectados con muestras de la misma familia de *software* dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.

– Conexión sospechosa: todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.

Obtención de información:

– Escaneo de puertos (*Scanning*): análisis local o remoto mediante *software*, del estado de los puertos de una máquina conectada a una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de red (*Scanning*): análisis local o remoto mediante *software*, del estado de una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de tecnologías: análisis local o remoto mediante *software*, de las tecnologías presentes o disponibles en una red determinada o un sistema de información concreto, mediante el cual se obtienen las referencias del *hardware/software* presente, así como su versión, y potenciales vulnerabilidades.

– Transferencia de zona DNS (AXFR IXFR): transacción de los servidores DNS utilizada para la replicación de las bases de datos entre un servidor primario y los secundarios. Estas transacciones pueden ser completas (AXFR) o incrementales (IXFR).

– Análisis de paquetes (*Sniffing*): análisis mediante *software* del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y leído por un atacante.

– Ingeniería social: técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

– *Phishing*: estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.

– *Spear Phishing*: variante del *phishing* mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

Intrusiones:

– Explotación: cualquier práctica mediante la cual un atacante cibernético vulnera un sistema de información y/o comunicación, con fines ilícitos o para los cuales no está debidamente autorizado.

– Inyección SQL: tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

– *Cross Site Scripting* XSS (Directo o Indirecto): ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

– *Cross Site Request Forgery* (CSRF): falsificación de petición en sitios cruzados. Es un tipo de *exploit* dañino de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el *Cross Site Request Forgery* explota la confianza que un sitio tiene en un usuario en particular.

– *Defacement*: tipología de ataque a sitios web en el que se implementa un cambio en la apariencia visual de la página. Para ello suelen emplearse técnicas como inyecciones SQL o algún tipo de vulnerabilidad existente en la página o en el servidor.

– Inclusión de ficheros (RFI y LFI): vulnerabilidad que permite a un atacante mostrar o ejecutar archivos remotos alojados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos. La inclusión local de archivos (LFI) es similar a la vulnerabilidad de Inclusión de archivos remotos, excepto que en lugar de incluir archivos remotos solo se pueden incluir archivos locales, es decir, archivos en el servidor actual para su ejecución.

– Evasión de sistemas de control: proceso por el cual una muestra de software dañino, o un conjunto de acciones orquestadas por un atacante cibernético, consiguen vulnerar o esquivar los sistemas o políticas de seguridad establecidas por un determinado sistema de información y comunicación.

– *Pharming*: ataque informático que aprovecha vulnerabilidades de los servidores DNS (*Domain Name System*). Al tratar de acceder el usuario al sitio web, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

– Ataque por fuerza bruta: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de todas las combinaciones posibles, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Ataque por diccionario: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Robo de credenciales de acceso: acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.

Disponibilidad:

– DoS (*Denial of Service*) o ataque de denegación de servicio: conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar

los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que este no puede atenderlas, provocando su colapso.

- DDoS (*Distributed Denial of Service*) o denegación distribuida de servicio: variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de *bots*, generalmente sin el conocimiento de los usuarios.

- Mala configuración: fallo de configuración en el *software* que está directamente asociado con una pérdida de disponibilidad de un servicio.

- Sabotaje/Terrorismo/Vandalismo: ataques implementados con el objetivo de provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes cometidos con propósitos ideológicos, políticos o religiosos.

- Disrupción sin intención dañina: acciones que pueden provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes.

- Inundación SYN o UDP: procedimientos usados para la realización de ataque DoS o DDoS consistente en iniciar una gran cantidad de sesiones impidiendo al servidor atender las peticiones lícitas.

- DNS *Open-Resolver*: servidor DNS capaz resolver consultas DNS recursivas procedentes de cualquier origen de Internet. Este tipo de servidores suele emplearse por usuarios malintencionados para la realización de ataques DDoS.

Compromiso de la información:

- Acceso no autorizado a la información o ciberespionaje: proceso por el cual un usuario no autorizado accede a consultar contenido para el cual no está autorizado.

- Modificación no autorizada de información: proceso por el cual un usuario no autorizado accede a modificar contenido para el cual no está autorizado.

- Borrado no autorizado de información: proceso por el cual un usuario no autorizado accede a borrar contenido para el cual no está autorizado.

- Exfiltración de información: proceso por el cual un usuario difunde información en canales o fuentes en las cuales no está prevista o autorizada la compartición de esa información.

- Acceso no autorizado a sistemas: proceso por el cual un usuario accede sin vulnerar ningún servicio, sistema o red, a sistemas de información y/o comunicación para los cuales no está debidamente autorizado, o no tiene autorización tácita o manifiesta.

- Ataque POODLE / Ataque FREAK: proceso por el que se consigue que un servidor haga uso de un protocolo de comunicaciones no seguro, que originalmente no estaba previsto, con el objetivo de poder exfiltrar información.

Fraude:

- Uso no autorizado de recursos: empleo de tecnologías y/o servicios por usuarios que no están debidamente autorizados por la Dirección o negociado competente.

- Suplantación de identidad: actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.

- Derechos de propiedad intelectual: la propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

- Otros fraudes: engaño económico con la intención de conseguir un beneficio, y con el cual alguien resulta perjudicado.

Vulnerabilidades:

- Tecnología vulnerable: conocimiento por parte de los administradores de tecnologías, servicios o redes, de vulnerabilidades presentes en estas.

- Política de seguridad precaria: política de seguridad de la organización deficiente, mediante la cual existe la posibilidad de que durante un espacio de tiempo determinado, atacantes cibernéticos realizaron accesos no autorizados a sistemas de información, no pudiendo determinar fehacientemente este extremo.

Otros:

– Ciberterrorismo: delitos informáticos previstos en los artículo 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal cuando dichos delitos se cometan con las finalidades previstas en el artículo 573.1 del mismo texto. Estas finalidades son:

- Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

- Alterar gravemente la paz pública.
- Desestabilizar gravemente el funcionamiento de una organización internacional.
- Provocar un estado de terror en la población o en una parte de ella.

– Daños informáticos PIC: delitos informáticos previstos en los artículos 264.2 3.º y 4.º de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relacionadas con el borrado, dañado, alteración, supresión, o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una Infraestructura Crítica. Así como conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

– APT (*Advanced Persistent Threat* o Amenaza Persistente Avanzada)/AVT (*Advanced Volatility Threat*): ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

– Dominios DGA: procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y Control, técnica usada en redes *Botnet* para dificultar su detención.

– Criptografía: técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.

– Proxy: ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera transparente para el usuario.

General:

– Ciberseguridad: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Ciberespacio: espacio virtual que engloba todos los sistemas TIC. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

– Redes y sistemas de información: se entiende por este concepto uno de los tres siguientes puntos:

- Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.

- Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados anteriormente para su funcionamiento, utilización, protección y mantenimiento.

– Seguridad en redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

§ 10 Desarrolla el Real Decreto-ley de seguridad de las redes y sistemas de información

- Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.
- Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Proveedor de servicios digitales: persona jurídica que presta un servicio digital.
- Ciberincidente: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.
- Gestión de ciberincidentes: todos los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante este.
- Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.
- Taxonomía: clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.
- RGPD: Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- OpenPGP: estándar basado en el programa PGP, del inglés *Pretty Good Privacy*, cuya finalidad es proteger la información mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.
- *Webinject*: herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios *web*.
- Telnet: protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
- RDP (*Remote Desktop Protocol*): protocolo propietario que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor.
- VNC (*Virtual Network Computing*): programa de software libre basado en una estructura cliente-servidor que permite observar remotamente las acciones del ordenador servidor a través de un ordenador cliente.
- SNMP (*Simple Network Management Protocol*): protocolo de red utilizado para el intercambio de mensajes para la administración de dispositivos en red.
- Redis: motor de base de datos en memoria, basado en el almacenamiento en tablas de *hashes*.
- ICMP (*Internet Control Message Protocol*): protocolo de control de mensajes de Internet.
- Copia de seguridad limpia: punto de restauración de un sistema de la que se tiene la seguridad de no estar comprometida.

§ 11

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems*)», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

- a) Seguridad como proceso integral.
- b) Gestión de la seguridad basada en los riesgos.
- c) Prevención, detección, respuesta y conservación.
- d) Existencia de líneas de defensa.
- e) Vigilancia continua.
- f) Reevaluación periódica.
- g) Diferenciación de responsabilidades.

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 9. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

- a) El responsable de la información determinará los requisitos de la información tratada
- b) El responsable del servicio determinará los requisitos de los servicios prestados.
- c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.

5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
- c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 27. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

- a) Los activos que constituyen los sistemas de información concernidos.
- b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
- c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurren impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team*), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team*, en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoría de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Disposición adicional primera. *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de dicha Secretaría de Estado.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

Disposición transitoria única. *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

- a) Confidencialidad [C].
- b) Integridad [I].
- c) Trazabilidad [T].
- d) Autenticidad [A].
- e) Disponibilidad [D].

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

- 1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño menor en los activos de la organización.
- 3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
- 4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
- 5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

- 1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño significativo en los activos de la organización.
- 3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
- 4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
- 5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

- 1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
- 2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
- 3.º El incumplimiento grave de alguna ley o regulación.
- 4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- 5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

ANEXO II

Medidas de Seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

- a) Las dimensiones de seguridad relevantes en el sistema a proteger.
- b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

- a) Identificación de los tipos de activos presentes.
- b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
- c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
- d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
- e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
		BAJO	MEDIO	ALTO
		Categoría de seguridad del sistema		
		BÁSICA	MEDIA	ALTA
org Marco organizativo				
org.1 Política de seguridad	Categoría	aplica	aplica	aplica
org.2 Normativa de seguridad	Categoría	aplica	aplica	aplica

ÁMBITOS DE LA SEGURIDAD NACIONAL: CIBERSEGURIDAD

§ 11 Esquema Nacional de Seguridad

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
		BAJO	MEDIO	ALTO	
		Categoría de seguridad del sistema			
		BÁSICA	MEDIA	ALTA	
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	Marco operacional				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
		BAJO	MEDIO	ALTO	
		Categoría de seguridad del sistema			
		BÁSICA	MEDIA	ALTA	
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

- [org.1.1] Los objetivos o misión de la organización.
- [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
- [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
- [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

- Categoría BÁSICA: org.1.
- Categoría MEDIA: org.1.
- Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

- [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: org.2.
- Categoría MEDIA: org.2.
- Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- [org.3.1] Cómo llevar a cabo las tareas habituales.
- [org.3.2] Quién debe hacer cada tarea.
- [org.3.3] Cómo identificar y reportar comportamientos anómalos.
- [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

- a) Su control de acceso.
- b) Su almacenamiento.
- c) La realización de copias.
- d) El etiquetado de soportes.
- e) Su transmisión telemática.
- f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

- Categoría BÁSICA: org.3.
- Categoría MEDIA: org.3.
- Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

- [org.4.1] Utilización de instalaciones, habituales y alternativas.
- [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- [org.4.3] Entrada de aplicaciones en producción.
- [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
- [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
- [org.4.6] Utilización de soportes de información.
- [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
- [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

- Categoría BÁSICA: org.4.
- Categoría MEDIA: org.4.
- Categoría ALTA: org.4.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

- [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
- [op.pl.1.2] Identifique las amenazas más probables.
- [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

- [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r1.2] Cuantifique las amenazas más probables.
- [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

- [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r2.2] Cuantifique las amenazas posibles.
- [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
- [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.1.
- Categoría MEDIA: op.pl.1 + R1.
- Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

- [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
- [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
- [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

§ 11 Esquema Nacional de Seguridad

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.2.
- Categoría MEDIA: op.pl.2 + R1.
- Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

- [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
- [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
- [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.3.
- Categoría MEDIA: op.pl.3.
- Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

- [op.pl.4.1] Necesidades de procesamiento.
- [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- [op.pl.4.3] Necesidades de comunicación.
- [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
- [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

- [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
- [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

- Nivel BAJO: op.pl.4.
- Nivel MEDIO: op.pl.4 + R1.
- Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

- [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.pl.5.
- Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

§ 11 Esquema Nacional de Seguridad

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.

– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

- Nivel BAJO: op.acc.1.
- Nivel MEDIO: op.acc.1 +R1.
- Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.2.
- Nivel MEDIO: op.acc.2.
- Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.

– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

§ 11 Esquema Nacional de Seguridad

Refuerzo R1-Segregación rigurosa.

- [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunar funciones de configuración y mantenimiento del sistema.
- [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

- [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

- [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.acc.3.
- Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
- [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
- [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.4.
- Nivel MEDIO: op.acc.4.
- Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A
-------------	---------

§ 11 Esquema Nacional de Seguridad

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

- [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
- [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
- [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
- [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
- [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
- [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
- [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
- [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
- [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

- [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.
- [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

- [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

- [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
- [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

- [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
- [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

§ 11 Esquema Nacional de Seguridad

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

- [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
- [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
- Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
- Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.

– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.

– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).

– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.

– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.

– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.

b) El tráfico deberá ser cifrado.

§ 11 Esquema Nacional de Seguridad

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.

d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
- Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
- Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: op.exp.1.
- Categoría MEDIA: op.exp.1.
- Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

- [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
- [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.

b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.

c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.

– Categoría MEDIA: op.exp.2.

– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).

– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).

– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).

– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).

– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).

– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.

– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.

– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.

– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

§ 11 Esquema Nacional de Seguridad

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.3.
- Categoría MEDIA: op.exp.3 + R1.
- Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

- [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
- [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
- [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

§ 11 Esquema Nacional de Seguridad

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).

3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.4.
- Categoría MEDIA: op.exp.4 + R1.
- Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

- [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.

- [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.

- [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.

- [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.

- [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

- [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.

- [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.

- [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.exp.5.
- Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.

- [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
- [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
- [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
- [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
- [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

- [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

- [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

- [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

- [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

- [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
- [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.6.
- Categoría MEDIA: op.exp.6+ R1 + R2.
- Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

- [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
- [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.

– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.

b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.

– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.

– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.

– Categoría MEDIA: op.exp.7+ R1 + R2.

– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

§ 11 Esquema Nacional de Seguridad

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.

– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.

– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.

– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.

– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.9.
- Categoría MEDIA: op.exp.9.
- Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

- [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
- [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
- [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

- [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

- [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.10.
- Categoría MEDIA: op.exp.10 + R1.
- Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.1.
- Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

§ 11 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

- [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
- [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.2.
- Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

- [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
- [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
- [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

- [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
- [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

- [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

- [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: no aplica.
- Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

§ 11 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.4.
- Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.

– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

- a) Auditoría de pruebas de penetración (*pentesting*).
- b) Transparencia.
- c) Cifrado y gestión de claves.
- d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

§ 11 Esquema Nacional de Seguridad

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

- Categoría BÁSICA: op.nub.1.
- Categoría MEDIA: op.nub.1 + R1.
- Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.cont.1.
- Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

- [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
- [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
- [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

- a) Servicios contratados a terceros.
- b) Instalaciones alternativas.
- c) Personal alternativo.
- d) Equipamiento informático alternativo.
- e) Medios de comunicación alternativos.

- [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.

- [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

- [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

§ 11 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

- [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

- [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

- [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

- [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.1.
- Categoría MEDIA: op.mon.1 + R1.
- Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

- [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

- [op.mon.2.r1.1] Se recopilarán los datos precisos que permitan evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

- [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.2.
- Categoría MEDIA: op.mon.2 + R1+ R2.
- Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

aplica + R1+R2 + R1+R2+R3+R4+R5+R6

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.

– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.

– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.

– [op.mon.3.r6.2] Análisis de vulnerabilidades.

– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.

– Categoría MEDIA: op.mon.3 + R1 + R2.

– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

§ 11 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
- [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.1.
- Categoría MEDIA: mp.if.1.
- Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.2.
- Categoría MEDIA: mp.if.2.
- Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

- [mp.if.3.1] Las condiciones de temperatura y humedad.
- [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
- [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.3.
- Categoría MEDIA: mp.if.3.
- Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

§ 11 Esquema Nacional de Seguridad

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.4.
- Nivel MEDIO: mp.if.4 + R1.
- Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.5.
- Nivel MEDIO: mp.if.5.
- Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.if.6.
- Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

§ 11 Esquema Nacional de Seguridad

- Categoría BÁSICA: mp.if.7.
- Categoría MEDIA: mp.if.7.
- Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.

– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.per.1.
- Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

- [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
- [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
- [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
- [mp.per.2.4] En caso de personal contratado a través de un tercero:
 - [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
 - [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

§ 11 Esquema Nacional de Seguridad

- [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.2.
- Categoría MEDIA: mp.per.2 + R1.
- Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

- [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.3.
- Categoría MEDIA: mp.per.3.
- Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

- a) Configuración de sistemas.
- b) Detección y reacción ante incidentes.
- c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.4.
- Categoría MEDIA: mp.per.4.
- Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

§ 11 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.1.
- Categoría MEDIA: mp.eq.1 + R1.
- Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.eq.2.
- Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

- [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
- [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

§ 11 Esquema Nacional de Seguridad

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.3.
- Categoría MEDIA: mp.eq.3.
- Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

- a) Dispositivos multifunción: impresoras, escáneres, etc.
- b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
- c) Dispositivos internet de las cosas, en inglés *Internet of Things (IoT)*.
- d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device (BYOD)*.
- e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.eq.4.
- Nivel MEDIO: mp.eq.4 + R1.
- Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
- [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

- Categoría BÁSICA: mp.com.1.
- Categoría MEDIA: mp.com.1.
- Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

- [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

- [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

- [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

- [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

- [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

- [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.com.2.

- Nivel MEDIO: mp.com.2 + R1.
- Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

- [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).

- [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

- a) La alteración de la información en tránsito.
- b) La inyección de información espuria.
- c) El secuestro de la sesión por una tercera parte.

- [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

- [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

- [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

- [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

- [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

- [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.com.3.
- Nivel MEDIO: mp.com.3 + R1 + R2.
- Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+ [R1oR2oR3]	+ [R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

Quando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

- [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
- [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

- [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
- [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

- Usuarios.
- Servicios.
- Administración.

Refuerzo R2-Segmentación lógica avanzada.

- [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

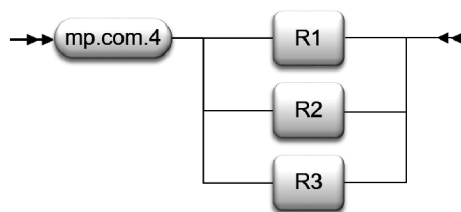
- [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

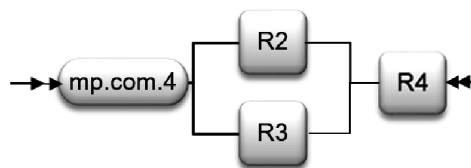
- [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
- [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



- Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

§ 11 Esquema Nacional de Seguridad

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.

– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.

– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.si.1.
- Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias de seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.si.2.
- Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

§ 11 Esquema Nacional de Seguridad

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

- [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
- [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

- Categoría BÁSICA: mp.si.3.
- Categoría MEDIA: mp.si.3.
- Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

- [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
- [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
- [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
- [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

- Categoría BÁSICA: mp.si.4.
- Categoría MEDIA: mp.si.4.
- Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

- [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

- [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

- [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.si.5.
- Nivel MEDIO: mp.si.5 + R1.
- Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

- [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

- [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

- [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:
 - a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
 - b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
 - c) Tratará específicamente los datos usados en pruebas.
 - d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

- [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:
 - a) Los mecanismos de identificación y autenticación.
 - b) Los mecanismos de protección de la información tratada.
 - c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

- [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

- [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
- Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

- [mp.sw.2.1] Se comprobará que:
 - a) Se cumplen los criterios de aceptación en materia de seguridad.
 - b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

- [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

- [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

- Categoría BÁSICA: mp.sw.2.
- Categoría MEDIA: mp.sw.2 + R1.
- Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.info.1.
- Categoría MEDIA: mp.info.1.
- Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

- [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
- [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.info.2.
- Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

- [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

- [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

- [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

- [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.info.3.
- Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
- Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

- [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
- [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
- [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
- [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

- [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
- [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

§ 11 Esquema Nacional de Seguridad

- Nivel BAJO: mp.info.5.
- Nivel MEDIO: mp.info.5.
- Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

- [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.

- [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

- a) Frecuencia de las copias.
- b) Requisitos de almacenamiento en el propio lugar.
- c) Requisitos de almacenamiento en otros lugares.
- d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

- [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

- [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

- Nivel BAJO: mp.info.6.
- Nivel MEDIO: mp.info.6+ R1.
- Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
- [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

- [mp.s.1.3] Correo no solicitado, en su expresión inglesa «spam».
- [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
- [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «applet».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

- [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
- [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.1.
- Categoría MEDIA: mp.s.1.
- Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+[R1oR2]	+[R1oR2]	+R2+R3

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

- [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).

c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.

d) Se prevendrán ataques de inyección de código.

- [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.

- [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

- [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.

- [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

- [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.

- [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.

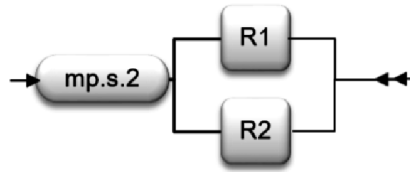
- [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

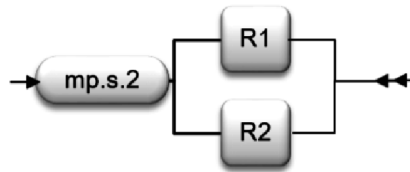
- [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

- Categoría BÁSICA: mp.s.2 + [R1 o R2].



- Categoría MEDIA: mp.s.2 + [R1 o R2].



- Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
- [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
- [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
- [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
- [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
- [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
- [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

- [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
- [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

- [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.3.
- Categoría MEDIA: mp.s.3.
- Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS* y *Distributed Denial of Service, DDoS*). Para ello:

- [mp.s.4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
- [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

- [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
- [mp.s.4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

- [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.s.4.
- Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM*) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, éstas se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostos. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

- a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
- b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
- c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
- d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

- a) Documentación de los procedimientos.
- b) Registro de incidentes.
- c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
- d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.

El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.

b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

§ 11 Esquema Nacional de Seguridad

- Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.
- Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.
- Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.
- Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.
- Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.
- Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.
- Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.
- Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.
- Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.
- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Dispositivo de autenticación (*token*): autenticador físico.
- Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.
- Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.
- Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:
 - a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
 - b) Servidor central (host), frontal Unix y equipos administrativos.
 - c) Seguridad física, seguridad lógica.
- Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

- Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.
- Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.
- Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.
- Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.
- Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.
- Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.
- Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.
- Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.
- PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.
- Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.
- Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
- Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.
- Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

§ 11 Esquema Nacional de Seguridad

- Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.
- Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.
- Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.
- Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.
- Sistema de información: cualquiera de los elementos siguientes:
 - 1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
 - 2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
 - 3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.
- TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.
- USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.
- Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

§ 12

Orden ESS/775/2014, de 7 de mayo, por la que se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social

Ministerio de Empleo y Seguridad Social
«BOE» núm. 117, de 14 de mayo de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-5111

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el derecho de los ciudadanos a relacionarse con las administraciones públicas a través de medios electrónicos, comportando una obligación para éstas de promover las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

Dicha ley determina que el Esquema Nacional de Seguridad tendrá por objeto establecer la política de seguridad en la utilización de medios electrónicos y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, entiende por seguridad un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Esta disposición reglamentaria obliga a todos los órganos superiores de las administraciones públicas a disponer formalmente de su política de seguridad, comprometiendo a todos los miembros de la organización.

En base a tales previsiones normativas, se dictaron la Orden TIN/3016/2011, de 28 de octubre, por la que se creó el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden comunicada de la Ministra de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

La Secretaría de Estado de la Seguridad Social, órgano superior del Ministerio de Empleo y Seguridad Social, ha establecido mediante Resolución de 2 de septiembre de 2013, de la Secretaría de Estado de la Seguridad Social, por la que se aprueba la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social, su política de seguridad identificando unos claros responsables de velar por su cumplimiento. La proliferación de los sistemas de información de los organismos adscritos y de los órganos dependientes de la Secretaría de Estado y la interconexión entre ellos, hace aconsejable la creación de un Comité de Seguridad de los Sistemas de Información en el ámbito de la Seguridad Social, como órgano colegiado con funciones de coordinación de aquéllos y de propuesta y aprobación de las medidas conducentes al cumplimiento de la política de seguridad a que obliga el Esquema Nacional de Seguridad.

§ 12 Comité de Seguridad de los Sistemas de Información de la Seguridad Social

En la tramitación de esta orden se ha obtenido el informe favorable del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Creación y adscripción del Comité de Seguridad de los Sistemas de Información de la Seguridad Social.*

Se crea el Comité de Seguridad de los Sistemas de Información de la Seguridad Social (en adelante CSISS) como órgano colegiado adscrito a la Secretaría de Estado de la Seguridad Social.

Artículo 2. *Funciones.*

El CSISS coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito de la Secretaría de Estado y se comunicará con el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Empleo y Seguridad Social (en adelante CSTIC), ejerciendo las siguientes funciones:

1. Definir y elevar para su aprobación al CSTIC los planes estratégicos, líneas de actuación y objetivos en materia de seguridad en la Secretaría de Estado de la Seguridad Social, siempre alineados con la misión y objetivos de la organización.

2. Garantizar la divulgación de la política de seguridad en el ámbito de la Secretaría de Estado de la Seguridad Social.

3. La aprobación y seguimiento de las normas y procedimientos en materia de seguridad que afecten transversalmente a la Administración de la Seguridad Social.

4. Establecer, cuando sea posible, criterios comunes de actuación en todos los órganos directivos de la organización para el cumplimiento de las normas o procedimientos en materia de seguridad de la información que sean de aplicación.

5. Revisar el estado global de la seguridad en cada uno de los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado, y elevar los informes pertinentes al CSTIC cuando sea necesario.

6. Trasladar las directrices que sean establecidas desde el CSTIC a cada uno de los órganos directivos y garantizar su cumplimiento.

7. Actualizar y asignar las funciones y obligaciones de cada uno de los responsables definidos en la política de seguridad en la utilización de medios electrónicos en la Administración de la Seguridad Social.

8. Promover las líneas de trabajo para una adecuada concienciación y formación en materia de seguridad para el personal de la Secretaría de Estado de la Seguridad Social.

9. Ser informado, deliberar e intercambiar información con los organismos adscritos y órganos y unidades dependientes orgánicamente de la Secretaría de Estado y que sean responsables de ficheros con datos personales para tratar y asesorar sobre las medidas de seguridad técnica aplicables en los sistemas y servicios que les afecten y que utilicen tecnologías de la información y comunicaciones.

Artículo 3. *Composición.*

El CSISS estará compuesto por los siguientes miembros:

1. Presidente: El Secretario de Estado de la Seguridad Social o persona que le sustituya.

2. Vocales: un representante designado por los titulares de cada uno de los siguientes órganos:

a) Gabinete de la Secretaría de Estado de la Seguridad Social.

b) Dirección General de Ordenación de la Seguridad Social.

c) Intervención General de la Seguridad Social.

d) Instituto Nacional de la Seguridad Social.

e) Tesorería General de la Seguridad Social.

f) Instituto Social de la Marina.

g) Servicio Jurídico de la Administración de la Seguridad Social.

h) Gerencia de Informática de la Seguridad Social.

Estos vocales deberán tener rango de subdirector general o asimilado, entendiéndose también por tales quienes ejerzan competencias en materia de seguridad de los sistemas de información en los órganos anteriores.

3. Secretaría: Con voz y sin voto, será designada por la Gerencia de Informática de la Seguridad Social.

Artículo 4. *Funcionamiento.*

El CSISS se reunirá con carácter ordinario como mínimo tres veces al año o, con carácter extraordinario, cuando el Presidente lo considere necesario.

En caso de ser necesario, y por invitación del Presidente del CSISS, podrán asistir en calidad de asesores, con voz pero sin voto, las personas que se estimen convenientes.

En todo caso, se aplicará con carácter supletorio lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición adicional única. *No incremento del gasto público.*

La creación y el funcionamiento del Comité de Seguridad de los Sistemas de Información de la Seguridad Social serán atendidos con los medios personales, técnicos y presupuestarios asignados a la Secretaría de Estado de la Seguridad Social.

Disposición final única. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 13

Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad

Ministerio de la Presidencia y para las Administraciones Territoriales
«BOE» núm. 20, de 23 de enero de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-799

El Consejo de Seguridad Nacional, en su reunión de 1 de diciembre de 2017, ha adoptado un Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad.

Para general conocimiento, y en cumplimiento de lo dispuesto en el apartado segundo del propio Acuerdo, se dispone su publicación como Anejo a la presente Orden.

ANEJO

Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad

Exposición

La disposición transitoria única de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, dispone que los Comités Especializados del Consejo de Seguridad Nacional existentes a su entrada en vigor, continuarán desarrollando sus funciones de acuerdo con los respectivos acuerdos de constitución hasta que sean adaptados a lo dispuesto en la misma.

Por otra parte, la Ley de Seguridad Nacional, además de asignar funciones concretas a los órganos competentes de la Seguridad Nacional, entre los cuales se encuentran las Cortes Generales, el Gobierno, el Presidente del Gobierno, los Ministros, el Consejo de Seguridad Nacional, los Delegados del Gobierno en las Comunidades Autónomas y en las ciudades con Estatuto de Autonomía de Ceuta y Melilla, así como los órganos que correspondan de las distintas Comunidades Autónomas según lo dispuesto en los respectivos Estatutos de Autonomía en conexión con las competencias relacionadas con la Seguridad Nacional y las autoridades locales, configura el concepto, las funciones y la estructura del Sistema de Seguridad Nacional con plena observancia del orden constitucional, tal como ha señalado el Tribunal Constitucional en la sentencia de 3 de noviembre de 2016.

Precisamente es en la estructura del Sistema de Seguridad Nacional donde los órganos de apoyo del Consejo de Seguridad Nacional hallan la razón de su existencia, como órganos dependientes del Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional al que corresponde asistir al Presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional y en las demás funciones que el ordenamiento jurídico le atribuya.

El carácter instrumental de los órganos de apoyo del Consejo de Seguridad Nacional ya existentes de acuerdo con la regulación contenida en el Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, se consolida en la Ley de Seguridad Nacional que, en concreto, en su artículo 20.3, prevé que estos órganos de apoyo con la denominación de Comités Especializados u otra que se determine, ejercen las funciones asignadas por el Consejo de Seguridad Nacional en los ámbitos de actuación previstos en la Estrategia de Seguridad Nacional, o cuando las circunstancias propias de la gestión de crisis lo precisen.

Para facilitar el ejercicio de las funciones del Consejo de Seguridad Nacional en el campo concreto de la ciberseguridad, al que la Ley de Seguridad Nacional considera un ámbito de especial interés para la Seguridad Nacional, cuyos objetivos y líneas de acción se han concretado en la Estrategia de Ciberseguridad Nacional, y así cumplir con el mandato de la Disposición transitoria única, siguiendo asimismo las directrices para la regulación de los órganos de apoyo del Consejo de Seguridad Nacional dictadas por el citado Consejo en el Acuerdo de 20 de enero de 2017, es necesario actualizar el Acuerdo de 5 de diciembre de 2013, por el que se adopta la iniciativa para la creación del Comité Especializado de Ciberseguridad, constituido bajo la denominación de Consejo Nacional de Ciberseguridad.

En particular, la puesta al día abarcará lo relacionado con su naturaleza jurídica, el régimen jurídico aplicable, las funciones específicas, la composición y, concretamente, el régimen de su presidencia y procedimiento de designación de sus miembros, además de otras previsiones, como la emisión de informes y finalidad de los mismos, la creación de grupos de trabajo y, por último, el reforzamiento del enlace y coordinación con los componentes fundamentales y ámbitos de especial interés para la Seguridad Nacional dentro del marco del Sistema de Seguridad Nacional de conformidad con lo dispuesto en el Acuerdo del Consejo de 20 de enero de 2017, de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional.

En su virtud, en aplicación de lo dispuesto en la Disposición transitoria única de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, en conexión con el artículo 21.1.h) de dicha Ley, y de conformidad con el Acuerdo del Consejo de Seguridad Nacional de 20 de enero de 2017, por el que se dictan directrices para la regulación de los órganos de apoyo, el Consejo de Seguridad Nacional, en su reunión del día 1 de diciembre de 2017, ha adoptado el siguiente Acuerdo:

ACUERDO

Primero.

Se modifica el marco regulador del Consejo Nacional de Ciberseguridad aprobado por Acuerdo del Consejo de Seguridad Nacional en su reunión del día 5 de diciembre de 2013, que queda redactado en la forma en que se recoge en el anexo al presente Acuerdo.

Segundo.

Este Acuerdo se publicará en el «Boletín Oficial del Estado», en la página web del Departamento de Seguridad Nacional www.dsn.gob.es y en las sedes electrónicas de los órganos y organismos a los que sea de aplicación y producirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Acuerdo por el que se regula el Consejo Nacional de Ciberseguridad

Primero. Objeto.

El presente Acuerdo tiene por objeto establecer el marco regulador del Consejo Nacional de Ciberseguridad (en adelante el Consejo) de conformidad con lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional y en las demás normas que resulten

de aplicación, en su condición de órgano de apoyo del Consejo de Seguridad Nacional en el marco del Sistema de Seguridad Nacional.

Segundo. *Naturaleza jurídica.*

El Consejo es un órgano de apoyo del Consejo de Seguridad Nacional de los previstos en el artículo 20.3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, al que corresponde ejercer las funciones asignadas por aquel en el ámbito de la ciberseguridad y en el marco del Sistema de Seguridad Nacional, según se concretan en este Acuerdo.

Tercero. *Régimen jurídico aplicable.*

El Consejo se rige por lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, por el presente Acuerdo y por sus Normas de régimen interno y de funcionamiento. En su defecto, por lo dispuesto en las instrucciones que han de seguirse para la tramitación de asuntos ante los órganos colegiados del Gobierno y en la legislación básica sobre régimen jurídico del sector público, que resulte de aplicación.

Cuarto. *Funciones específicas.*

El Consejo ejercerá las siguientes funciones:

1. Proponer al Consejo de Seguridad Nacional las directrices en materia de planificación y coordinación de la política de Seguridad Nacional relacionadas con la ciberseguridad.
2. Contribuir a reforzar el adecuado funcionamiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad, cuya supervisión y coordinación corresponde al Consejo de Seguridad Nacional.
3. Apoyar al Consejo de Seguridad Nacional en su función de verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y proponer, en su caso, su revisión, en lo relacionado con la ciberseguridad.
4. Verificar el grado de cumplimiento de la Estrategia de Ciberseguridad Nacional, así como de los instrumentos de desarrollo aprobados, para ulterior informe al Consejo de Seguridad Nacional, con propuestas para una posible revisión de la existente o aprobación de una nueva estrategia sectorial.
5. Contribuir a la elaboración de propuestas normativas para el fortalecimiento del Sistema de Seguridad Nacional en el ámbito de la ciberseguridad.
6. Apoyar la toma de decisiones del Consejo de Seguridad Nacional en las materias propias del ámbito de la ciberseguridad, mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
7. Reforzar las relaciones con las Administraciones Públicas concernidas en el ámbito de la ciberseguridad, así como la coordinación, colaboración y cooperación entre los sectores público y privado.
8. Realizar en apoyo del Comité Especializado de Situación la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, en especial de aquellos susceptibles de derivar en una situación de interés para la Seguridad Nacional, en el ámbito de la ciberseguridad, y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes y con el Comité Especializado de Situación.
9. Contribuir a la organización de la contribución de recursos a la Seguridad Nacional de responsabilidad del Consejo de Seguridad Nacional en el ámbito de la ciberseguridad.
10. Aprobar sus propias normas de régimen interno y de funcionamiento.
11. Todas aquellas otras funciones que le atribuya el ordenamiento jurídico o que le encomiende el Consejo de Seguridad Nacional.

Quinto. *Composición.*

a) Presidencia:

La presidencia será ejercida por el Secretario de Estado Director del Centro Nacional de Inteligencia.

Corresponde al Presidente:

§ 13 Consejo Nacional de Ciberseguridad

- Ostentar la representación del órgano y, en particular, canalizar los informes del Consejo Nacional de Ciberseguridad para el Consejo de Seguridad Nacional.
- Acordar la convocatoria de las sesiones ordinarias y extraordinarias y la fijación del orden del día en los términos señalados en las Normas de régimen interno y de funcionamiento.
- Presidir las reuniones, moderar el desarrollo de los debates y acordar su suspensión por causas justificadas.
- Asegurar el cumplimiento de las leyes.
- Visar las actas y certificaciones de los acuerdos del órgano.
- Velar por la búsqueda del consenso para la adopción de acuerdos.
- En caso de llevarse a cabo votación para la adopción de un acuerdo, de conformidad con las Normas de régimen interno y de funcionamiento, dirimirá con su voto los empates.
- Las demás funciones previstas en las normas legales y reglamentarias que resulten aplicables y, en particular, en las Normas de régimen interno y de funcionamiento del Consejo.

b) Vicepresidencia:

La Vicepresidencia será ocupada por el Director del Departamento de Seguridad Nacional.

Corresponderá al Vicepresidente sustituir al Presidente en los casos de vacante, ausencia, enfermedad u otra causa legal, y en su defecto, por el miembro de mayor jerarquía, antigüedad y edad, por este orden.

c) Vocales:

1. El Comité estará compuesto por un vocal con rango mínimo de Subdirector general o asimilado u Oficial General de cada departamento ministerial y organismo público con representación en el Consejo de Seguridad Nacional, que será designado por el titular del ministerio y organismo respectivo.

2. Asimismo, podrá formar parte del Consejo un representante del resto de los departamentos ministeriales u organismos públicos cuya presencia sea así acordada por el Presidente, en función de los asuntos a tratar.

3. Serán convocados, además, los titulares de los órganos superiores y directivos de la Administración General del Estado, las autoridades competentes de las Comunidades Autónomas, de las ciudades con Estatuto de Autonomía, de la Administración Local, así como de los organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas, cuando su contribución se considere necesaria y, en todo caso, cuando los asuntos a tratar afecten a sus respectivas competencias. Igualmente, podrán ser convocados representantes de las demás entidades que integran el sector público institucional, del sector privado y aquellas personas en su condición de expertos cuya contribución se considere relevante.

4. El Consejo podrá ser convocado por el Presidente en composición reducida de acuerdo con las circunstancias concurrentes y el orden del día fijado para la reunión.

5. Los miembros del Consejo no podrán atribuirse las funciones de representación asignadas en su condición de órgano de apoyo, salvo que expresamente se les hayan reconocido por una norma o por acuerdo expresamente así adoptado para cada caso en particular, por el propio Consejo.

d) Secretaría Técnica y órgano de trabajo permanente del Consejo y otros apoyos a la presidencia:

1. Las funciones de Secretaría Técnica y órgano de trabajo permanente del Consejo serán desempeñadas por el Departamento de Seguridad Nacional. En este campo, le corresponderá efectuar la coordinación necesaria para que el Consejo en el ámbito de sus funciones preste el apoyo necesario al Consejo de Seguridad Nacional, asumiendo, en este contexto, el punto de enlace único entre el citado Consejo y el presente órgano de apoyo.

2. El Secretario será designado por el Presidente, a propuesta del Director del Departamento de Seguridad Nacional, entre el personal perteneciente a dicho Departamento.

3. En apoyo a la presidencia, el Presidente podrá recabar los apoyos necesarios de su propia estructura, en especial en todo lo relacionado con la organización de las reuniones del Consejo, bajo la coordinación del Departamento de Seguridad Nacional.

Sexto. *Emisión de informes.*

1. Los informes únicamente podrán ser emitidos a instancia del Consejo de Seguridad Nacional o a iniciativa del propio Consejo.

2. En todo caso, serán elevados a la consideración y, en su caso, conformidad del Consejo de Seguridad Nacional, a través del Presidente.

Séptimo. *Utilización de los mecanismos de enlace y coordinación.*

1. El Consejo utilizará los mecanismos de enlace y coordinación que en cumplimiento a lo dispuesto en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, ha establecido el Consejo de Seguridad Nacional en el Acuerdo de 20 de enero de 2017, de implementación de los mecanismos para garantizar el funcionamiento integrado del Sistema de Seguridad Nacional, así como aquellos otros que se determinen en cumplimiento de lo dispuesto en la mencionada Ley.

2. De acuerdo con lo dispuesto en el apartado quinto del citado Acuerdo del Consejo de Seguridad Nacional de 20 de enero de 2017, los miembros del Consejo velarán por la coherencia y armonización de la información a trasladar en el seno del Consejo, para lo cual se coordinarán con sus respectivos puntos de contacto de Seguridad Nacional, dando así cumplimiento a los principios y procedimientos de actuación previstos en el mencionado Acuerdo.

3. El Departamento de Seguridad Nacional, de acuerdo con lo establecido en el artículo 20.4 de la Ley 36/2015, de 28 de septiembre, mantendrá activados los mecanismos de enlace y coordinación permanentes con los organismos del conjunto de las Administraciones Públicas que sean necesarios para que el Sistema de Seguridad Nacional ejerza sus funciones y cumpla con sus objetivos, de manera continua y sin perjuicio de las funciones que correspondan al Comité Especializado de Situación en materia de gestión de crisis.

Octavo. *Grupos de trabajo.*

1. El Consejo podrá crear grupos de trabajo para la asistencia técnica en el desempeño de sus funciones, con la composición, objetivos, cometidos y calendario para su realización, que para cada caso se disponga. Los grupos de trabajo podrán incorporar a expertos en la materia o recabar su criterio e invitar a participar en sus actividades a representantes de las Administraciones Públicas y del sector público y privado.

2. Los grupos de trabajo responderán ante el Consejo del resultado de sus cometidos y actividades que desarrollen, y serán coordinados por el Departamento de Seguridad Nacional.

3. El régimen de funcionamiento de los grupos de trabajo que se constituyan se determinará en las normas de régimen interno de las que se doten. En lo no previsto, se tendrá en cuenta lo dispuesto en la Sección 3.ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Noveno. *Reuniones.*

El Consejo se reunirá con carácter presencial o a distancia a iniciativa de su Presidente como mínimo con carácter bimestral, o cuantas veces lo considere oportuno, atendiendo a las circunstancias que en materia de ciberseguridad demande la Seguridad Nacional, todo ello de acuerdo con lo dispuesto en este Acuerdo y en las Normas de régimen interno y de funcionamiento del Consejo.

§ 14

Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad
«BOE» núm. 103, de 30 de abril de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-6347

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia Nacional de Ciberseguridad 2019.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

ANEXO

Estrategia Nacional de Ciberseguridad 2019

Sumario

Presidencia del Gobierno.
Consejo de Seguridad Nacional.
Sumario.
Resumen ejecutivo.
Introducción.
Capítulo 1: El ciberespacio como espacio común global.
El ciberespacio: oportunidades y desafíos.
Infraestructura digital.
Plano internacional: seguridad en el ciberespacio.
Una nueva concepción del ciberespacio.
Capítulo 2: Las amenazas y desafíos en el ciberespacio.
Ciberamenazas.
Acciones que usan el ciberespacio para fines maliciosos.
Capítulo 3: Propósito, principios y objetivos para la ciberseguridad.
Propósito.
Principios Rectores.
Objetivo general.
Objetivo I.
Objetivo II.
Objetivo III.
Objetivo IV.

Objetivo V.

Capítulo 4: Líneas de acción y medidas.

Línea de acción 1.

Línea de acción 2.

Línea de acción 3.

Línea de acción 4.

Línea de acción 5.

Línea de acción 6.

Línea de acción 7.

Capítulo 5: La ciberseguridad en el Sistema de Seguridad Nacional.

El Consejo de Seguridad Nacional.

El Comité de Situación.

El Consejo Nacional de Ciberseguridad.

La Comisión Permanente de Ciberseguridad.

Foro Nacional de Ciberseguridad.

Autoridades públicas competentes y los CSIRT de referencia nacionales.

Consideraciones finales y evaluación.

Resumen ejecutivo

La Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

El documento se estructura en cinco capítulos. El primero, titulado «El ciberespacio, más allá de un espacio común global», proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio una de los principales riesgos para nuestro desarrollo como nación.

Por ello, la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

Contribuir a la promoción de un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podemos enfrentar, incluyendo nuevas y emergentes.

El segundo capítulo, titulado «Las amenazas y desafíos en el ciberespacio» determina las principales amenazas del ciberespacio que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

El tercer capítulo, titulado «Propósito, principios y objetivos para la ciberseguridad» aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos. Su desarrollo, se plasma en el cuarto capítulo titulado «Líneas de acción y medidas», donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio;

impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El quinto capítulo, titulado «La ciberseguridad en el Sistema de Seguridad Nacional» define la arquitectura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el foro Nacional de Ciberseguridad.

Asimismo, en este último capítulo, se exponen a modo de conclusión, unas consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la Estrategia.

Introducción

La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. El documento fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone, para el país, la vulnerabilidad del ciberespacio. Además, la estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional. Igualmente, en estos años, España ha seguido avanzando en sus esfuerzos por contribuir a la promoción de un ciberespacio seguro y fiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional. Desde su primera reunión, el Consejo Nacional de Ciberseguridad ha asumido la tarea de coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad y sus planes derivados. Así, hoy España cuenta con organismos especializados en ciberseguridad y una posición destacada a nivel europeo e internacional.

El marco jurídico también ha experimentado una notable adaptación. En respuesta a su evolución y a la experiencia acumulada en estos años, en 2015 se publicó la modificación del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del Sector Público. Por otro lado, la entrada en vigor del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS), ha supuesto un importante hito en la mejora de la ciberseguridad en nuestro país, extendiendo el alcance de esta Directiva con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional se promulgó con vocación de dar impulso a uno de los proyectos de mayor responsabilidad para un gobierno, la Seguridad Nacional. La Ley de Seguridad Nacional contempla la ciberseguridad como ámbito de especial interés.

Se puede afirmar, sin lugar a dudas, que la ciberseguridad ha modernizado la Seguridad Nacional, tratándose de uno de los ámbitos de mayor avance hasta la fecha. Esta dinámica debe seguir su camino adelante.

La Estrategia de Seguridad Nacional 2017 marca un punto de inflexión en el pensamiento estratégico nacional, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

Ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, y para el que la colaboración público-privada es un elemento clave, resulta necesaria una nueva aproximación, una nueva estrategia nacional de ciberseguridad.

CAPÍTULO 1

El ciberespacio como espacio común global

Este capítulo presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter inherentemente internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

El ciberespacio: oportunidades y desafíos:

El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

Por una parte, el ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Se constituye así en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. La inteligencia artificial, la robótica, el big data, el blockchain y el internet de las cosas son ya una realidad, si bien el verdadero potencial transformador está todavía por descubrir. Sus implicaciones van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

Por otra parte, la digitalización transforma la seguridad y presenta serios desafíos. El ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo. Así, la creciente conectividad y la mayor dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales, generan vulnerabilidades y dificultan la adecuada protección de la información.

Infraestructura digital:

Además de su naturaleza virtual, el ciberespacio se sustenta en elementos físicos y lógicos. Los dispositivos, componentes y sistemas que constituyen las redes y sistemas de información y comunicaciones están expuestos a disfunciones que alteran su correcto funcionamiento y a acciones deliberadas con fines malintencionados, que ponen en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas.

Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

Todos estos elementos, unidos a la creciente interconectividad entre sistemas pueden originar efectos en cascada con resultados impredecibles.

Plano internacional: seguridad en el ciberespacio:

La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza. En este contexto, España defiende su visión e intereses como nación y contribuye al esfuerzo conjunto de la comunidad internacional en su apuesta por un ciberespacio abierto, plural y seguro.

España continúa participando activamente en todas las instituciones en las que la ciberseguridad ocupa un lugar destacado, en especial en el marco de la Unión Europea, la Alianza Atlántica y de Naciones Unidas, demostrando así el compromiso con sus socios y aliados. Asimismo, se mantienen vínculos con terceros Estados mediante mecanismos de cooperación bilateral que facilitan elementos de entendimiento y confianza mutua basados en las relaciones fluidas en el ámbito de la ciberseguridad y orientados hacia la construcción de capacidades.

Consciente de la importancia del multilateralismo, además del Derecho Internacional y las normas no vinculantes de comportamiento responsable de los Estados, se destaca el papel de La Carta de Naciones Unidas como principio de referencia para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio. La construcción de consensos y las medidas de fomento de confianza constituyen la base para su aplicación y puesta en práctica, así como los Tratados y Convenios Internacionales en los que España es parte.

Una nueva concepción del ciberespacio:

Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.

El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado.

En primer lugar, el sector privado juega un papel relevante como uno de los gestores y propietarios de los activos digitales de España, por lo que las capacidades de ciberseguridad del país residen en gran medida en las de sus empresas. Es por tanto necesario el apoyo, la promoción y la inversión en ciberseguridad para impulsar la competitividad y el crecimiento económico, a la vez que proporcionar un entorno digital seguro y fiable.

Por otra parte, se debe aspirar a incrementar la autonomía tecnológica mediante el fomento de una base industrial nacional de ciberseguridad, la I+D+i y la gestión del talento tecnológico. En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento o de formación requerida.

En segundo lugar, la transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore elementos de mayor fuerza disuasoria obedece a un contexto global de mayor competencia geopolítica. El empleo del ciberespacio como dominio de confrontación, de forma independiente o como parte de una acción híbrida, es un

rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.

En tercer lugar, la rápida evolución de las ciberamenazas aconseja una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones. Así mismo, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución.

A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.

CAPÍTULO 2

Las amenazas y desafíos en el ciberespacio

En este capítulo se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España.

La promoción de un entorno seguro y fiable es una tarea que debe partir del conocimiento y la comprensión de los desafíos y las amenazas, incluyendo las nuevas y emergentes que afectan al ciberespacio. La Estrategia de Seguridad Nacional de 2017 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

Ciberamenazas:

Las ciberamenazas son todas aquellas interrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

Su carácter transversal, exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

En este escenario, las defensas deben evolucionar continuamente para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto llamada que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

En este sentido, la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Acciones que usan el ciberespacio para fines maliciosos:

Las tecnologías digitales dan entrada a nuevas actividades y formas de negocio que requieren ser debidamente reguladas, pues pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Igualmente, las mismas cualidades que hacen del ciberespacio un motor del progreso, pueden ser explotadas con fines perniciosos al sumarse a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación.

Debido a la revolución de Internet, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable

en otros tiempos. La conectividad digital lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada.

Las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas incluyen las relacionadas con el ciberespionaje y la cibercriminalidad.

El ciberespionaje es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional, dada la dificultad de atribución de la autoría. Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas (APT). Un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción para ejecutar sus objetivos.

Asimismo, se constata una tendencia creciente de las denominadas amenazas híbridas, acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.

La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término Cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos.

CAPÍTULO 3

Propósito, principios y objetivos para la ciberseguridad

En este capítulo se establece el propósito y los principios por los que se rige la Estrategia, así como los objetivos: uno general y cinco específicos.

Propósito:

España precisa, tal y como establece la Estrategia de Seguridad Nacional de 2017, garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable.

Por tanto, el propósito de la Estrategia Nacional de Ciberseguridad 2019, es fijar las directrices generales del ámbito de la ciberseguridad de manera que se alcancen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

Para ello, España ha de seguir avanzando en el refuerzo de capacidades para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio. En consecuencia, se seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

Por otra parte, el fomento de la cultura de ciberseguridad ha de ser uno de los ejes centrales a desarrollar a fin de contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida.

Asimismo, la ciberseguridad es progreso, por lo que el apoyo e impulso de la industria española de ciberseguridad, la promoción de un entorno que favorezca la investigación, el desarrollo y la innovación, y la participación del mundo académico tiene un carácter singular. Por otro lado, es un objetivo prioritario en nuestra sociedad alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas y profesionales, ya que solo mediante su promoción se podrá responder a los grandes retos de la ciberseguridad.

La transversalidad y globalidad del ciberespacio, requiere además de la cooperación y del cumplimiento del Derecho internacional, del máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas; en coherencia con la Estrategia de Seguridad Nacional y con las iniciativas desarrolladas en el marco europeo, regional e internacional, prevaleciendo en todo momento los intereses nacionales.

Principios rectores:

La Estrategia Nacional de Ciberseguridad, se sustenta y se inspira en los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia.

Unidad de Acción: Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

Una gestión centralizada de las crisis que afecten al ciberespacio, permite mantener una visión completa de la situación de la amenaza y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

Anticipación: La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente deber participar el sector privado.

La anticipación prima las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, con información compartida lo más próximo al tiempo real, permite alcanzar un adecuado conocimiento de la situación. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas.

Eficiencia: La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación. A lo anterior se suma la necesidad de una planificación anticipada y una elevada complejidad en su sostenimiento.

Además, el escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los dedicados a la ciberseguridad, por lo que resultarán indispensables la unidad de acción, compartición de información e integración de estos recursos para alcanzar la eficiencia deseada.

Resiliencia: La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas. Especial mención merece el refuerzo que requieren las redes de información y comunicaciones frente a actividades de las ciberamenazas o al uso ilícito del ciberespacio.

Objetivo general:

Los nuevos retos de la ciberseguridad han requerido la adaptación de su objetivo general de manera que se muestre más integrador, inclusivo y menos tecnificado.

En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Basados en este objetivo general, a continuación, se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito.

Objetivo I

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

Es necesario consolidar un marco nacional coherente e integrado que ayude a garantizar la protección de la información manejada por el sector público y por los servicios esenciales, sus sistemas y servicios, así como de las redes que los soportan. Este marco permitirá desarrollar e implantar servicios cada vez más seguros y eficientes.

Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

En particular, las acciones contra el ciberespionaje merecen especial mención para asegurar la protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

El sector público y los operadores de servicios esenciales se deben involucrar activamente en un proceso de mejora continua respecto de la protección de sus sistemas de Tecnologías de la Información y las Comunicaciones basados en una vigilancia permanente

de su exposición a las amenazas. Estos agentes deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.

En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la Información y las Comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad.

El fortalecimiento de la ciberseguridad requiere un conocimiento sistemático sobre el impacto de una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales, así como métricas del nivel de seguridad de estos sistemas que permitan la oportuna toma de decisiones según su grado de exposición.

Objetivo II

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

El ciberespacio juega un papel cada vez más importante tanto en la comisión de hechos ilícitos o maliciosos como en su investigación para promover la confianza de los ciudadanos. Es necesario garantizar una adecuada persecución de los fenómenos criminales que en él se desarrollen.

Son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito.

Sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, así como la asignación de recursos suficientes a los órganos competentes en la materia y la capacitación de los profesionales que trabajan en este ámbito.

Del mismo modo, es fundamental fomentar la colaboración y participación ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés judicial y policial e identificando aspectos que requieran de una mejora en las capacidades de las instituciones policiales y de los organismos judiciales competentes.

Objetivo III

Protección del ecosistema empresarial y social y de los ciudadanos

Todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Es por ello responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ciberseguridad es una responsabilidad compartida con los actores privados que, por acción u omisión, puedan afectarla; y no es posible conseguirla sin su participación. Por tanto, entre las medidas a impulsar deben estar aquellas que conduzcan a la necesaria cooperación para la seguridad común.

La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa. A la vez todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance.

La acelerada adopción por la sociedad de tecnologías emergentes provoca que los riesgos evolucionen. Por ello, el intercambio permanente de conocimiento con los diferentes actores y el establecimiento de mecanismos de monitorización para la protección del ecosistema empresarial y social serán instrumentos que permitirán al Gobierno estar informado y tomar las decisiones oportunas para actualizar y adecuar las acciones resultado de la presente estrategia.

Objetivo IV

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con recursos técnicos y humanos que le proporcionen la autonomía tecnológica necesaria y la capacitación adecuada para el uso seguro del ciberespacio, situando a la ciberseguridad como habilitador clave para una nación emprendedora.

Para ello, debe mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas.

Se debe también contribuir al uso seguro y responsable de las Tecnologías de la Información y de las Comunicaciones promoviendo la capacitación en ciberseguridad de los profesionales adecuada a la demanda del mercado laboral, estimulando el desarrollo de los profesionales con habilidades propias, impulsando la formación y cualificación especializada, así como las capacidades de generación de conocimiento, el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados.

Asimismo, merece especial atención la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para promover la soberanía tecnológica y aprovechar las oportunidades que ofrece la transformación digital, se fomentará e impulsará la industria española de ciberseguridad y las mejores prácticas en el desarrollo e implantación de sistemas de información y comunicaciones.

Objetivo V

Seguridad del ciberespacio en el ámbito internacional

España promoverá un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado.

Abogará por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

En línea con nuestros socios europeos, reforzará la confianza en Internet, en la transformación digital y en el desarrollo de las nuevas tecnologías, contribuyendo a consolidar un ecosistema cibernético europeo seguro que permita avances hacia el mercado único digital. Para ello defenderá un internet interoperativo, neutral, abierto y diverso, reflejo de la pluralidad cultural y lingüística internacional, basado en un sistema de gobernanza democrático, representativo e inclusivo, resultado de la concertación y el consenso. Además, un acceso a internet global y generalizado, contribuyendo con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

Del mismo modo, nuestra pertenencia a la Unión Europea (UE), nos obliga a fortalecer la seguridad y la autonomía estratégica europea mediante la búsqueda de sinergias, la cooperación técnica, operativa, estratégica y política; a reforzar nuestra resiliencia, nuestra capacidad de respuesta ante las crisis y las complementariedades entre los ámbitos civiles y militares como socios de la UE y aliados de la Organización del Tratado del Atlántico Norte (OTAN).

Sobre la base de lo anterior, España continuará participando activamente en la UE y la OTAN; en Naciones Unidas, y en sus foros derivados como el Foro de Gobernanza de Internet (IGF); en la Organización para la Seguridad y la Cooperación en Europa (OSCE), en el desarrollo e implementación de las Medidas de Fomento de la Confianza; en la Organización de Estados Americanos (OEA). Así como con el Foro Global del Expertos en Ciberseguridad (GFCE) y la Coalición por la Libertad en Internet (Freedom Online Coalition. FOC), sin olvidar nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE), así como en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

Además, reforzará la cooperación internacional bilateral en materia de ciberseguridad, promoverá relaciones fluidas y de confianza en este ámbito, colaborará en la construcción de capacidades en terceros Estados, prestando especial atención a las mujeres y los jóvenes y fomentará la creación de canales de información e intercambio de experiencias, impulsando, para todo ello, la adopción de acuerdos bilaterales y multilaterales en este ámbito.

CAPÍTULO 4

Líneas de acción y medidas

En este capítulo se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio:

Esta línea de acción responde al Objetivo I de la Estrategia.

Medidas:

1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.

2. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.

3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.

4. Asegurar la coordinación técnica y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.

5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.

6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.

7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.

8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.

9. Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.

10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.

11. Garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.

12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España:

Esta línea de acción responde al Objetivo I de la Estrategia.

Medidas:

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
3. Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo.
4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.
6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.
7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permita a las autoridades competentes determinar el nivel de seguridad y su evolución.
8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.
9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.
10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.
11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad, especialmente en áreas que puedan afectar a la Seguridad Nacional, la Administración pública, los servicios esenciales y las empresas cotizadas.
12. Asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i.

Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio:

Esta línea de acción responde al Objetivo II de la Estrategia.

Medidas:

1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.
3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.
4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.

5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.

6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.

7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

8. Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.

9. Fortalecer la cooperación judicial y policial internacional.

Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas:

Esta línea de acción responde al Objetivo III de la Estrategia.

Medidas:

1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.

3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la «identidad digital».

4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.

5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implantarán medidas de ciberdefensa activa de ciudadanos y pymes.

6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.

7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.

8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.

9. Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

Línea de Acción 5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital:

Esta línea de acción responde al Objetivo IV de la Estrategia.

Medidas:

1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.

2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.

3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.

4. Promover las actividades de normalización y la exigencia de requisitos ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.

5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.

8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.

9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales:

Esta línea de acción responde al Objetivo V de la Estrategia.

Medidas:

1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales y a los que pertenece y en los que la ciberseguridad forma parte sustancial de sus agendas, y apoyar y participar de manera activa en las diferentes iniciativas, coordinando la posición de los diferentes agentes nacionales implicados.

2. Promover en el ámbito de Naciones Unidas la búsqueda de consensos para el pleno respeto a la Carta de Naciones Unidas y la aplicación y puesta en práctica del Derecho Internacional y las normas para el comportamiento responsable de los Estados. Y del mismo modo avanzar en la adopción e implementación de Medidas para el Fomento de la Confianza en el ciberespacio.

3. Participar activamente en la Unión Europea en el desarrollo de un ecosistema europeo seguro que favorezca el avance y la consolidación del mercado único, y la seguridad y autonomía estratégica de Europa, buscando las complementariedades y la cooperación entre la Unión Europea y la OTAN.

4. Fomentar el diálogo bilateral, la cooperación y los sistemas de intercambio de información, alerta temprana y de experiencias para desarrollar un enfoque coordinado en la lucha contra las ciberamenazas con otros países, promoviendo la negociación y firma de acuerdos internacionales.

5. Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

6. Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países.

Línea de Acción 7. Desarrollar una cultura de ciberseguridad:

Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al objetivo IV de la Estrategia.

Medidas:

1. Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.

2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.
4. Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.
5. Promover un espíritu crítico en favor de una información veraz y de calidad y que contribuya a la identificación de las noticias falsas y la desinformación.
6. Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.
7. Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.
8. Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

CAPÍTULO 5

La ciberseguridad en el Sistema de Seguridad Nacional

En este capítulo se contempla la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015 establecen una estructura orgánica específica para la ciberseguridad. En la presente Estrategia de 2019 se impulsan iniciativas que complementan los nuevos avances en el modelo de gobernanza nacional con las políticas europeas.

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

El Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

El Consejo de Seguridad Nacional actúa, a través del Departamento de Seguridad Nacional como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

El Comité de Situación:

El Comité de Situación tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.

El Consejo Nacional de Ciberseguridad:

El Consejo Nacional de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Entre sus funciones se encuentran reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilitar la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto

en el ámbito nacional como en el internacional, así como realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

La Comisión Permanente de Ciberseguridad:

La Comisión Permanente de Ciberseguridad se establece con objeto de facilitar la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.

El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis en el ámbito de la ciberseguridad. Dicho procedimiento establece sus funciones dirigidas a detectar y valorar los riesgos y amenazas; facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, e instrucciones para la gestión de la comunicación pública.

A fin de responder de manera oportuna y proporcionada a situaciones de especial relevancia en el desarrollo de sus funciones, se progresará en la definición de sus capacidades y responsabilidades.

Foro Nacional de Ciberseguridad:

Actuará en la potenciación y creación de sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas a la seguridad en el ciberespacio.

La puesta en marcha del foro Nacional de Ciberseguridad, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

Autoridades públicas competentes y los CSIRT de referencia nacionales:

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacional que se recogen en el marco jurídico nacional.

Asimismo, los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y sus organismos vinculados o dependientes, los de las entidades privadas, la red de CSIRT.es y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos. De igual modo, desde los CSIRT nacionales, en colaboración con los CSIRT autonómicos y privados, se fomentará la puesta en marcha de iniciativas que contribuyan a la consecución de los objetivos de la estrategia nacional.

Consideraciones finales y evaluación:

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en el presente documento una actualización de las amenazas y los desafíos a las que nos enfrentamos, siempre en continua evolución. Para adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Se elaborará un informe

anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

§ 15

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos

Ministerio del Interior
«BOE» núm. 224, de 18 de septiembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-10060

El Reglamento de protección de infraestructuras críticas aprobado por el Real Decreto 704/2011, de 20 de mayo, por el que se desarrolla la Ley 8/2011, de 28 de abril, en la que se establecen medidas para la protección de las infraestructuras críticas, dispone en los artículos 22.4 y 25.5 que la Secretaría de Estado de Seguridad establecerá, respectivamente, los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos comprendidos en el artículo 14 de la Ley.

Dichos contenidos mínimos fueron recogidos en la Resolución de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, resolución a su vez modificada por otra, de 29 de noviembre de 2011, que advertía y corregía determinados errores en la primera.

La constante evolución de la amenaza, la implantación de nuevas regulaciones, estrategias y herramientas de planificación, así como la experiencia adquirida en los últimos cuatro años, en buena parte, merced a las aportaciones efectuadas por los propios operadores críticos, hacen aconsejable la actualización de tales contenidos mínimos, con el fin de adecuar el nivel de planificación y respuesta a las exigencias requeridas para una eficaz protección de las infraestructuras críticas nacionales.

En virtud de ello, y conforme a lo preceptuado en el artículo 7, apartado e), del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, resuelvo aprobar y ordenar la publicación en el «Boletín Oficial del Estado» de los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos que se insertan como anexo I y anexo II, respectivamente, de esta resolución.

La presente resolución deroga la precedente en esta misma materia, de la Secretaría de Estado de Seguridad, de 15 de noviembre de 2011, por la que se establecían los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, así como también la de 29 de noviembre de 2011, que modificaba la anterior.

ANEXO I

Guía Contenidos Mínimos

Plan de Seguridad del Operador (PSO)

Índice

1. Introducción.
 - 1.1 Base Legal.
 - 1.2 Objetivo de este Documento.
 - 1.3 Finalidad y Contenido del PSO.
 - 1.4 Método de Revisión y Actualización.
 - 1.5 Protección y Gestión de la Información y Documentación.
 2. Política General de Seguridad del Operador y Marco de Gobierno.
 - 2.1 Política General de Seguridad del Operador Crítico.
 - 2.2 Marco de Gobierno de Seguridad.
 - 2.2.1 Organización de la Seguridad y Comunicación.
 - 2.2.2 Formación y Concienciación.
 - 2.2.3 Modelo de Gestión Aplicado.
 - 2.2.4 Comunicación.
 3. Relación de Servicios Esenciales prestados por el Operador Crítico.
 - 3.1 Identificación de los Servicios Esenciales.
 - 3.2 Mantenimiento del Inventario de Servicios Esenciales.
 - 3.3 Estudio de las Consecuencias de la Interrupción del Servicio Esencial.
 - 3.4 Interdependencias
 4. Metodología de Análisis de Riesgos.
 - 4.1 Descripción de la Metodología de Análisis.
 - 4.2 Tipologías de Activos que Soportan los Servicios Esenciales.
 - 4.3 Identificación y Evaluación de Amenazas.
 - 4.4 Valoración y Gestión de Riesgos.
 5. Criterios de aplicación de medidas de seguridad integral.
 6. Documentación complementaria.
 - 6.1 Normativa, Buenas Prácticas y Regulatoria.
 - 6.2 Coordinación con Otros Planes.
1. Introducción.
 - 1.1 Base legal.

El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada, cuyo funcionamiento es indispensable y no permite soluciones alternativas: las denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población.

Este es precisamente el espíritu de la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que tiene como objeto el establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, impulsando la colaboración e implicación de los organismos y/o empresas gestoras

y propietarias (operadores críticos) de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados tanto físicos como lógicos, que puedan afectar a la prestación de los servicios esenciales.

Dicha Ley tiene su desarrollo a través del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El artículo 13 de la Ley explicita una serie de compromisos para los operadores críticos públicos y privados, entre los que se encuentra la necesidad de elaboración de un Plan de Seguridad del operador (en adelante, PSO) y de los Planes de Protección Específicos que se determinen (en adelante, PPE).

Por su parte, el artículo 22.4 del Real Decreto 704/2011 responsabiliza a la Secretaría de Estado de Seguridad (órgano superior responsable del Sistema de Protección de Infraestructuras Críticas Nacionales, conforme al artículo 6 de la Ley 8/2011), a través del CNPIC, del establecimiento y puesta a disposición de los operadores críticos de los contenidos mínimos con los que deben contar los PSO, así como el modelo en el que basar la elaboración de los mismos.

1.2 Objetivo de este Documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe de apoyar un operador crítico a la hora del diseño y elaboración de su PSO. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia.

Igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que estos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los PPE de cada una de sus infraestructuras críticas.

1.3 Finalidad y contenido del PSO.

El PSO definirá la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

El PSO, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá, además de un índice referenciado sobre los contenidos del Plan, información sobre:

- Política general de seguridad del operador y marco de gobierno.
- Relación de Servicios Esenciales prestados por el operador crítico.
- Metodología de análisis de riesgo (amenazas físicas y de ciberseguridad).
- Criterios de aplicación de Medidas de Seguridad Integral.

1.4 Método de revisión y actualización

Conforme al artículo 24 del Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador, además de la elaboración y presentación del PSO al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante CNPIC), se incluye su revisión y actualización periódica:

- Revisión: Bienal.
- Actualización: Cuando se produzca algún tipo de modificación en los datos incluidos en el PSO. En este caso, el PSO quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PSO (modificación de datos, identificación de nuevas infraestructuras críticas, baja de infraestructuras críticas, cese de condiciones para ser considerado operador crítico, etc...), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la información y documentación.

La información es un valor estratégico para cualquier organización, siendo ésta de carácter sensible, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de esa información, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la ley 08/2011, la clasificación del PSO constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PSO deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el Personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad Física.

OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Política General de Seguridad del Operador y Marco de seguridad.

2.1 Política General de Seguridad del Operador Crítico.

El objetivo de una Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad. En ella, la Dirección de la Organización debe establecer claramente cuáles son sus líneas de actuación y manifestar su apoyo y compromiso con la seguridad.

Por tanto, en este apartado, el operador deberá reflejar el contenido de su Política de Seguridad de una forma homogénea e integral que esté específicamente dirigido al ámbito de las infraestructuras críticas y que sirva de marco de referencia para la protección de las mismas, con el objetivo de impedir su perturbación o destrucción.

Los aspectos mínimos que debe recoger la Política de Seguridad son:

- Objeto: La meta que pretende conseguir la Organización con la política y su posterior desarrollo y aplicación.

- Ámbito o Alcance de Aplicación: Una política puede estar limitada a determinados campos o aspectos o, por el contrario, ser de aplicación a toda la Organización. El operador deberá reflejar sobre qué partes de su Organización es aplicable la Política de Seguridad de protección de infraestructuras críticas, sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la ciberseguridad.

- Compromiso de la Alta Dirección: El operador debe garantizar que a la seguridad debe dársele la misma importancia que a otros factores de la producción o negocio de la organización.

Por ello, el compromiso de la Organización con la Política de Seguridad y lo que de ella se desarrolle deberá quedar plasmado mediante la aprobación, sanción y apoyo de la misma

por el órgano (Consejo de Administración, Consejo de Dirección, etc.) o la persona (Presidente, Consejero Delegado, etc.) de gobierno o dirección de la misma con capacidad suficiente para implantarla en la organización, así como su firme y explícito compromiso con la protección de los servicios esenciales prestados, compromiso que se debe ver reflejado en el propio plan.

- **Carácter Integral de la Seguridad:** La seguridad física y la ciberseguridad son áreas que deben ser abordadas de forma interrelacionada y con una perspectiva holística de la seguridad. Esto redundará en una visión global de la seguridad, posibilitando el diseño de una estrategia corporativa única, y optimizando el conocimiento, los recursos y los equipos. Por ello, el operador deberá remarcar el carácter integral de la seguridad aplicada a sus infraestructuras críticas, indicando en todo caso el procedimiento por el que se pretende alcanzar dicha seguridad integral: aspectos concretos de la organización, estructuras, procedimientos, etcétera. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad física y ciberseguridad.

- **Actualización de la Política General de Seguridad del Operador:** Al ser la política de seguridad un documento de alto nivel, no suele requerir cambios significativos a lo largo del tiempo. No obstante, el operador deberá asegurarse de que ésta se mantenga actualizada y refleje aquellos cambios requeridos por variaciones en los activos a proteger, del entorno que les pueda afectar (amenazas, vulnerabilidades, impactos, salvaguardas), o en la reglamentación aplicable. En este apartado, el operador deberá recoger el proceso a seguir para la actualización y mantenimiento de su Política de Seguridad, incluyendo la periodicidad y el responsable de llevar a cabo estas acciones.

2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad y Comunicación.

El operador crítico debe designar a un Responsable de Seguridad y Enlace y a los Delegados de Seguridad en cada una de las infraestructuras críticas identificadas, así como a los sustitutos de ambos, de acuerdo a los requisitos establecidos en la Ley 8/2011. Deberá, por tanto, asegurar que se encuentren en un nivel jerárquico suficiente dentro de su estructura organizativa, de tal forma que los designados puedan garantizar el cumplimiento y la aplicación de la Política y de los requisitos establecidos para la protección de las infraestructuras críticas bajo su responsabilidad.

Asimismo, deberá asegurar la presencia física del delegado de seguridad en la infraestructura en un tiempo prudencial, en caso de que ello sea necesario.

En este apartado, el operador crítico deberá describir su organigrama de seguridad (comprendiendo tanto la Seguridad Física como la Ciberseguridad), con indicación de las figuras recogidas en la Ley, así como los niveles jerárquicos que les correspondan en su estructura organizativa.

Dicho organigrama debe incluir la ubicación física, estructura, jerarquía, órgano de gobierno e interrelación de todas las áreas de la organización con responsabilidad en cada uno de los ámbitos de la seguridad corporativa. Además, deberá dejar constancia de que los designados tienen capacidad suficiente para llevar a cabo todas aquellas acciones que se deriven de la aplicación de la Ley y el Real Decreto. En este sentido, el operador crítico deberá presentar:

- Un organigrama general, donde se identifique la estructura de seguridad corporativa.
- Un organigrama específico de la estructura de seguridad que integre la información sobre las distintas funciones que desempeña en la organización.

En su caso, el operador crítico deberá señalar los comités u órganos de decisión existentes en materia de seguridad, así como las funciones de cada uno de ellos.

Igualmente, se reflejarán los procedimientos de gestión y mantenimiento de la seguridad, haciendo constar si éstos son de carácter propio o son subcontratados. En este último caso, será necesario relacionar la empresa o empresas subcontratadas, las certificaciones en materia de seguridad con las que cuentan aquéllas, la sede desde la que se ejercen dichos servicios contratados, así como los servicios y compromisos acordados entre ambos. De igual forma, se definirá la metodología mediante la cual se lleva a cabo la comprobación del

cumplimiento por parte de la empresa contratada, con los protocolos de seguridad implementados en su caso por el operador.

En el campo de la ciberseguridad, y en lo relacionado con la protección de infraestructuras críticas, el CERT de Seguridad e Industria (en adelante CERTSI) es el responsable de la resolución de incidencias cibernéticas que puedan afectar a la prestación de los servicios esenciales gestionados por los

El CERTSI, en aplicación del Acuerdo Marco suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas y a la disponibilidad de los servicios que éstos prestan.

Para todo ello, y previa suscripción de un acuerdo de confidencialidad entre las partes (operador crítico – CNPIC – CERTSI), dicho CERT podrá proporcionar servicios de prevención, detección, alerta temprana y respuesta a incidentes en apoyo a los departamentos encargados de esta labor en el seno de cada organización.

2.2.1.1 El Responsable de Seguridad y Enlace.

Conforme al artículo 16.2 de la Ley, el operador crítico deberá nombrar, en el plazo de tres meses desde su designación como tal, al Responsable de Seguridad y Enlace de la organización, que deberá estar habilitado por el Ministerio del Interior como Director de Seguridad, en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, en el que se aprueba el Reglamento de Seguridad Privada, o tener una habilitación equivalente, según su normativa sectorial específica. Tal nombramiento deberá ser comunicado a la Secretaría de Estado de Seguridad, a través del CNPIC.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Responsable de Seguridad y Enlace así como de su sustituto, con idénticas condiciones, en ausencia del titular. Sus funciones en relación con el artículo 34.2 del Real Decreto 704/2011 son las siguientes:

- Representar al operador crítico ante la Secretaria de Estado de Seguridad:
 - En materias relativas a la seguridad de sus infraestructuras.
 - En lo relativo a los diferentes planes especificados en el Real Decreto.
- Canalizar las necesidades operativas e informativas que surjan entre el operador crítico y el CNPIC.

2.2.1.2 El Delegado de Seguridad de la Infraestructura Crítica.

Conforme al artículo 17 de la Ley, el operador crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la notificación oficial de que es propietario o gestor de al menos una infraestructura crítica o crítica europea.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad, así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación como operador crítico, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materias relativas a la seguridad de sus infraestructuras.

§ 15 Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

- Canalizar las necesidades operativas e informativas que surjan, a nivel infraestructura, entre el operador y las autoridades competentes.

2.2.2 Formación y Concienciación.

El operador crítico deberá colaborar con los programas o ejercicios que puedan derivarse del Plan Estratégico Sectorial, así como en su momento de los Planes de Apoyo Operativo.

El operador crítico reflejará en este apartado el Plan de Formación previsto para el personal relacionado con la protección de las infraestructuras críticas, indicando la duración, objetivos que se pretende conseguir, mecanismos de evaluación que se contemplan para el mismo y periodos de actualización. Así mismo, se incluirá el responsable del plan y la capacitación del mismo.

En el caso de que disponga de un Plan de Formación General, especificará la parte relacionada con la protección de las infraestructuras críticas, y la incluirá en este punto.

El operador crítico deberá reflejar en este apartado su participación en ejercicios de simulación en incidentes de seguridad (físicos y cibernéticos), y la periodicidad programada para tales ejercicios.

El personal implicado directamente en la protección de los servicios esenciales e infraestructuras críticas deberá ser formado para alcanzar conocimientos, a nivel básico:

- Sobre seguridad integral (seguridad física y ciberseguridad).
- Sobre autoprotección.
- Sobre seguridad del medio ambiente.
- Sobre habilidades organizativas y de comunicación.
- Sobre sus responsabilidades/actuaciones en caso de materializarse un incidente, o en el caso de que se active un nivel de amenaza 4 ó 5 del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

El personal no directamente implicado deberá ser concienciado mediante la aplicación de las políticas de formación y operacionales activas en la organización.

2.2.3 Modelo de Gestión aplicado.

La seguridad integral depende de un proceso de gestión que debe aportar el control organizativo y técnico necesario para determinar en todo momento el nivel de exposición a las amenazas y el nivel de protección y respuesta que es capaz de proporcionar la organización para la protección y seguridad de sus servicios esenciales e Infraestructuras Críticas.

Por tanto, de acuerdo con la Política de Seguridad marcada, el operador crítico deberá recoger dentro del PSO su modelo de gestión elegido, que deberá contemplar como mínimo:

- Una implementación de controles de seguridad alineada con las prioridades y necesidades evaluadas.
- Una evaluación y monitorización continua de la seguridad, con identificación de procesos y periodos.
- En el supuesto de que el operador crítico haya diseñado un sistema de gestión y/o la evaluación de la seguridad de las tecnologías de la información, de acuerdo a algún estándar de referencia internacional se debe indicar éste, así como las certificaciones que posee dicho sistema y el organismo certificador.

2.2.4 Comunicación.

El operador crítico deberá recoger explícitamente en este apartado los procedimientos establecidos para la comunicación e intercambio de información relativa a la protección de infraestructuras críticas, de la siguiente manera:

Comunicación al CNPIC:

- De aquellos incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de alguna de las infraestructuras de la que el operador es gestor y/o propietario, conforme al protocolo de comunicación de incidentes PIC elaborado por este Centro y puesto a disposición de los operadores críticos.

§ 15 Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

- De aquellas variaciones de carácter organizativo, de planificación o estructural que se produzcan en el seno del propio operador y que afecten de alguna manera a las infraestructuras críticas objeto de protección (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

Comunicación al CERTSI:

- A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes del operador crítico y la disponibilidad de los servicios que presta. Todo ello, conforme al protocolo de comunicación de incidentes PIC elaborado por el CNPIC y puesto a disposición de los operadores críticos.

3. Relación de Servicios esenciales prestados por el Operador Crítico.

El PSO deberá incluir, a modo de introducción, la información de contexto suficiente para describir los siguientes aspectos:

- Presentación general del operador crítico y sector/subsector principal/es de su actividad. En caso de grupos empresariales, se identificará claramente, con nombre y CIF, cuál de las empresas es el operador crítico.

- Estructura organizativa y societaria de todo el Grupo (en el caso de grupos empresariales).

- Presencia geográfica en los ámbitos nacional e internacional, con un resumen de las Comunidades Autónomas donde presten sus servicios esenciales, así como de aquellos países donde presten servicios similares.

- Principales líneas de actividad con la tipología general de servicios/productos que ofrecen.

3.1 Identificación de los Servicios esenciales.

El PSO deberá identificar aquellos servicios esenciales para la ciudadanía prestados por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional, en relación al concepto de servicio esencial recogido en el artículo 2. a) de la Ley:

- Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos.

- Eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

3.2 Mantenimiento del inventario de servicios esenciales.

Periódicamente, al menos bienalmente, el operador crítico deberá revisar la relación de servicios esenciales que figuran en su PSO, como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece.

Así, en este mantenimiento deberá incorporar aquellos cambio/s que se produzcan:

- Por causas endógenas (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

- Como consecuencia de la adecuación a los períodos establecidos en el Plan conforme al punto 1.4 de esta guía.

3.3 Estudio de las consecuencias de la interrupción del servicio esencial.

El operador crítico deberá llevar a cabo un estudio de las consecuencias que supondría la interrupción y no disponibilidad del servicio esencial que presta a la sociedad, motivado por:

- Alteración o interrupción temporal del servicio prestado.

- Destrucción parcial o total de la infraestructura que gestiona el servicio.

Adicionalmente, deberá identificar claramente, para cada uno de los casos anteriores, la siguiente información:

- Extensión geográfica y número de personas que pueden verse afectadas.

- Efecto sobre operadores y servicios esenciales dependientes.
- Existencia de alternativas de prestación del servicio esencial o mecanismos de contingencia proporcionados por el propio operador y nivel de degradación que conllevan.

3.4 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en otros sectores diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores en el marco global de su organización.

El operador crítico deberá hacer referencia a las interdependencias que identifique, explicando en líneas generales el motivo que origina dichas dependencias:

- Entre sus propias instalaciones o servicios.
- Con operadores del mismo sector.
- Con operadores de distintos sectores.
- Con operadores de otros países, del mismo sector o no.
- Con sus proveedores de servicio dentro de la cadena de suministros.
- Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.

4. Metodología del Análisis de Riesgos.

En virtud de lo establecido en el artículo 22.3 del Real Decreto 704/2011, en el PSO se plasmará la metodología o metodologías de análisis de riesgos empleadas por el operador crítico. Dichas metodologías deberán estar internacionalmente reconocidas, garantizar la continuidad de los servicios proporcionados por dicho operador y contemplar, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos críticos. Todo ello, con independencia de las medidas mínimas que se puedan establecer para los Planes de Protección Específicos conforme a lo establecido por el artículo 25.

4.1 Descripción de la metodología de análisis.

Se describirá de forma genérica la metodología empleada por la Organización para la realización de los análisis de riesgos de los diferentes Planes de Protección Específicos (PPE) que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

- Etapas esenciales.
- Algoritmos de cálculo empleados.
- Método empleado para la valoración de los impactos.
- Métricas de medición de riesgos aceptables, residuales, etc.
- En particular, se harán constar las relaciones entre los análisis de riesgos realizados a distintos niveles: A nivel de corporación, a nivel de servicios y el más concreto, a nivel de infraestructuras críticas.

4.2 Tipologías de activos que soportan los servicios esenciales.

Se denominan activos los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

Sobre la base de los servicios identificados en el apartado 3.1 anterior, se incluirán en este apartado, para cada servicio esencial, los tipos de activos que los soportan, diferenciando aquéllos que son críticos de los que no lo son.

Las tipologías de activos a considerar serán, al menos:

- Las instalaciones necesarias para la prestación del servicio esencial.

- Los sistemas informáticos necesarios para dar soporte a los servicios esenciales (hardware y software).
- Las redes de comunicaciones necesarias para la prestación del servicio esencial.
- Las personas que explotan u operan todos los elementos anteriormente citados.

El objeto de esta sección es la identificación genérica de tipologías de activos asociadas a los servicios esenciales prestados por dicho operador, y sobre los que se focalizará el análisis de riesgos que efectúe el operador. El nivel de detalle será aquel que permita una comprensión del funcionamiento de los servicios, así como las interrelaciones entre activos y servicios.

Los activos no serán necesariamente espacios físicos concretos, pudiendo por ejemplo considerarse como activos sistemas distribuidos, tales como una red de datos.

4.3 Identificación y evaluación de amenazas.

En el marco de la normativa de protección de infraestructuras críticas y de cara a garantizar la adecuada protección de aquellas infraestructuras que prestan servicios esenciales, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

- Las intencionadas, de tipo tanto físico como lógico, que puedan afectar al conjunto de sus infraestructuras, las cuales deberán identificarse de forma específica en sus respectivos PPE, en su caso.
- Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.

4.4 Valoración y Gestión de Riesgos.

Los PSO recogerán la estrategia de gestión de riesgos implementada por el operador en cuanto a:

- Criterios utilizados para la valoración de las categorías de clasificación de los riesgos.
- Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.).
- Plazos para la implantación de medidas, en el caso de elegir una estrategia de minimización del riesgo con indicación, si existe, de mecanismos de priorización de acciones.
- Tratamiento dado a las amenazas de ataques deliberados y, en particular, a aquellas que tengan una baja probabilidad pero un alto impacto debido a las consecuencias por su destrucción o interrupción en la continuidad de los servicios esenciales.
- Mecanismos de seguimiento y actualización periódicos de niveles de riesgo.

5. Criterios de aplicación de medidas de seguridad integral.

Dentro del ámbito de la seguridad integral, el operador definirá a grandes rasgos los criterios utilizados en su organización para la aplicación y administración de la seguridad. En este sentido, incluirá de forma genérica las medidas de seguridad implantadas en el conjunto de activos y recursos sobre los que se apoyan los servicios esenciales y que se recogerán en sus respectivos PPE, al objeto de hacer frente a las amenazas físicas y lógicas identificadas en los oportunos análisis de riesgos efectuados sobre cada una de las tipologías de sus activos.

6. Documentación complementaria.

6.1 Normativa, buenas prácticas y regulatoria.

El operador recogerá en una breve referencia motivada toda la normativa de aplicación y aquellas buenas prácticas que regulen el buen funcionamiento de los servicios esenciales prestados por todas y cada una de sus infraestructuras.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

- Seguridad Física.

- Ciberseguridad.
- Seguridad de la Información.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

6.2 Coordinación con otros Planes.

Se identificarán todos aquellos Planes diseñados por el operador relativos a otros aspectos (continuidad de negocio, gestión del riesgo, respuesta, ciberseguridad, autoprotección, emergencias, etc.) que puedan coordinarse con el Plan de Seguridad del operador y los respectivos Planes de Protección Específicos que serán activados en el caso de que las medidas preventivas fallen y se produzca un incidente. Así mismo, debe dejarse constancia de la coordinación existente con el Plan Nacional para la Protección de las Infraestructuras Críticas.

ANEXO II

Guía de contenidos mínimos

Plan de Protección Específico (PPE)

Índice

1. Introducción.
 - 1.1 Base Legal.
 - 1.2 Objetivo de este Documento.
 - 1.3 Finalidad y Contenido del PPE.
 - 1.4 Método de Revisión y Actualización.
 - 1.5 Protección y Gestión de la Información y Documentación.
2. Aspectos Organizativos.
 - 2.1 Organigrama de Seguridad.
 - 2.2 Delegados de Seguridad de las Infraestructuras Críticas.
 - 2.3 Mecanismos de Coordinación.
 - 2.4 Mecanismos y Responsables de Aprobación.
3. Descripción de la Infraestructura Crítica.
 - 3.1 Datos Generales de la infraestructura crítica.
 - 3.2 Activos/Elementos de la infraestructura crítica.
 - 3.3 Interdependencias.
4. Resultados del Análisis de Riesgos.
 - 4.1 Amenazas Consideradas.
 - 4.2 Medidas de Seguridad Integral existentes.
 - 4.2.1 Organizativas o de Gestión.
 - 4.2.2 Operacionales o Procedimentales.
 - 4.2.3 De Protección o Técnicas.
 - 4.3 Valoración de Riesgos.
5. Plan de Acción propuesto (por activo).
6. Documentación complementaria.
 1. Introducción.
 - 1.1 Base legal.

Según establece la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico, ya sea éste

perteneciente al sector público o al privado, se integrará como agente del sistema de protección de infraestructuras críticas, debiendo cumplir con una serie de responsabilidades recogidas en su artículo 13.

De acuerdo con en el punto 1, letra «d», del citado artículo, el operador deberá elaborar un Plan de Protección Específico (en adelante, PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, a través del cual se da desarrollo reglamentario a la Ley 8/2011, establece, en su capítulo IV del Título III sobre los Instrumentos de Planificación, aquellos aspectos relativos a la elaboración, finalidad y contenido de dichos planes, además de su aprobación o modificación, registro, clasificación y formas de revisión y actualización, así como las autoridades encargadas de su aplicación y seguimiento, y la compatibilidad con otros planes ya existentes.

En este sentido, y conforme al artículo 25.5 de dicho real decreto, se asigna a la Secretaría de Estado de Seguridad, a través del Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC), la responsabilidad de establecer los contenidos mínimos de los PPE, así como el modelo en el que fundamentar su estructura y compleción, sobre la base de las directrices y criterios marcados por el Plan de Seguridad del Operador (en adelante, PSO).

En el PPE, el operador crítico aplicará los siguientes aspectos y criterios incluidos en su PSO, que afecten de manera específica a esa instalación:

- Aspectos relativos a su política general de seguridad.
- Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica.
- Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como aquellas que afectan a la ciberseguridad, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

1.2 Objetivo de este documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe apoyar el operador crítico a la hora de elaborar su respectivo PPE en las instalaciones catalogadas como críticas. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la Ley 8/2011 y el Real Decreto 704/2011.

1.3 Finalidad y contenido del PPE.

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (seguridad física y ciberseguridad) de sus infraestructuras críticas.

Además de un índice referenciado a los contenidos del Plan, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

- Organización de la seguridad.
- Descripción de la infraestructura.
- Resultado del análisis de riesgos:

Medidas de seguridad integral (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional de acuerdo con lo establecido por el Plan de Prevención y Protección Antiterrorista y por el Plan Nacional de Protección de Infraestructuras Críticas.

- Plan de acción propuesto (por cada activo evaluado en el análisis de riesgos).

Los PPE deberán estar alineados con las pautas establecidas en la Política General de Seguridad del operador reflejada en el PSO. Así mismo, los análisis de riesgos, vulnerabilidades y amenazas que se lleven a cabo, estarán sujetos a las pautas metodológicas descritas en el PSO.

1.4 Método de Revisión y Actualización.

Conforme al artículo 27 del Real Decreto por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador crítico, además de la elaboración y presentación del PPE al CNPIC, se incluye su revisión y actualización periódica:

- Revisión: Bienal, que deberá ser aprobada por las Delegaciones del Gobierno en las CC.AA. y las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, además de por parte del CNPIC.

- Actualización: Cuando se produzca una modificación en los datos incluidos dentro del PPE. En este caso, el PPE quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PPE (organización de la seguridad, datos de descripción de la infraestructura, medidas de seguridad, etc...), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES/PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 Protección y Gestión de la Información y Documentación.

La información asociada con los PPE y aquella relativa a los análisis de riesgos y las medidas de seguridad implantadas sobre las infraestructuras críticas a las que hacen referencia es de carácter sensible, por lo que, en este sentido, el operador deberá definir sus procedimientos de tratamiento de dicha información, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de la información utilizados, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la Ley 08/2011, la clasificación del PPE constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PPE deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

Seguridad documental.

OR-ASIP-04-01.04.–Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

Seguridad en el personal.

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

Seguridad física.

OR-ASIP-01-01.03.–Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03.–Orientaciones para la Constitución de Zonas de Acceso Restringido.

Seguridad de los Sistemas de Información y Comunicaciones.

OR-ASIP-03-01.04.–Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. Aspectos organizativos.

2.1 Organigrama de seguridad.

El operador crítico debe presentar gráficamente la estructura organizativa funcional que en materia de seguridad integral existe en la infraestructura crítica, con indicación de todos los actores que participan en aquella, su rol de responsabilidad y su jerarquía en el proceso de toma de decisiones. Del mismo modo, se debe establecer la dependencia de esta estructura con aquella definida en el correspondiente Plan de Seguridad del Operador.

2.2 Delegados de Seguridad de las Infraestructuras Críticas.

Conforme al artículo 17 de la Ley 8/2011, el operador crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno en las CC.AA. y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquellas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la designación de una infraestructura como crítica.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad así como de su sustituto, con idénticas condiciones, cumpliendo los plazos establecidos desde su designación, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materia relativa a la seguridad de sus infraestructuras.
- Canalizar las necesidades operativas e informativas que surjan.

El operador crítico deberá reflejar en este apartado los cursos o formación que el Delegado de Seguridad haya recibido, relacionados con las habilidades necesarias para el desempeño del puesto, de acuerdo con el Plan de Formación previsto en el PSO.

2.3 Mecanismos de Coordinación.

El operador crítico deberá reflejar dentro de su PPE los mecanismos existentes de coordinación:

- Entre el Delegado de Seguridad de la infraestructura crítica con otros Delegados de otras infraestructuras críticas y con el Responsable de Seguridad y Enlace del propio operador.
 - Con autoridades y terceros (Fuerzas y Cuerpos de Seguridad del Estado/Cuerpos Policiales autonómicos y locales/CNPIC/otros).
 - Con otros planes existentes del operador (planes de continuidad de negocio, planes de evacuación, etc.).
 - Con el CERT de Seguridad e Industria (CERTSI) identificando los puntos de contacto del operador en los 3 niveles requeridos: el institucional, y el directivo y el técnico, todos ellos referidos a en la gestión de incidentes.
 - Con los proveedores críticos que se especifiquen a tenor del desarrollo de lo establecido en el punto 3.2.

2.4 Mecanismos y responsables de aprobación.

El operador deberá incluir dentro del PPE los siguientes aspectos relativos a su aprobación y revisión interna:

- Responsables de su aprobación.
- Procedimiento que se sigue para su aprobación.
- Fecha en la que se produjo su última aprobación.

§ 15 Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

- Responsable de su revisión y actualización.
- Aspectos objeto de revisión, en su caso.
- Registros generados por el procedimiento de revisión que permitan comprobar que el PPE ha sido revisado (reuniones, acta del Comité correspondiente, estudios y análisis realizados, actualizaciones de los análisis de riesgos, etc.).

3. Descripción de la Infraestructura Crítica.

3.1 Datos generales de la infraestructura crítica.

El operador crítico deberá incluir los siguientes datos e información sobre la infraestructura a proteger:

- Generales, relativos a la denominación y tipo de instalación, propiedad y gestión de la misma.
 - Sobre localización física y estructura (localización, planos generales, fotografías, componentes, etc.)
 - Sobre los sistemas TIC que gestionan la infraestructura crítica y su arquitectura.
 - Datos estratégicos:

Descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional del mismo.

Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.

Descripción de sus funciones y de su relación con los servicios esenciales soportados.

3.2 Activos/elementos de la infraestructura críticas.

Se incluirán en este apartado todos los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

- Las instalaciones o componentes de la infraestructura crítica que son necesarios y por lo tanto vitales para la prestación del servicio esencial.
- Los sistemas informáticos (hardware y software) utilizados, con especificación de los fabricantes, modelos y, versiones, etcétera.
- Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha infraestructura crítica:

Arquitectura de red, rangos de IP públicas y, dominios.

Esquema(s) de red completo y detallado, de tipo gráfico y con descripción literaria, donde se recojan los flujos de intercambio de información que se realizan en las redes, así como sus perímetros electrónicos.

Descripción de componentes de la red (servidores, terminales, hubs, switches, nodos, routers, firewalls,...) así como su ubicación física.

- Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados, indicando y detallando de forma particular si existe algún proceso externalizado a terceros.
- Los proveedores críticos que en general son necesarios para el funcionamiento de dicha infraestructura crítica, y específicamente:

De suministro eléctrico.

De comunicaciones (telefonía, internet, etc. ...).

De tratamiento y almacenamiento de información (CPDs, etc.).

De ciberseguridad (CERTs privados, SOCs, etc.).

- Sobre los proveedores nombrados por el operador, se especificarán los distintos Acuerdos de Nivel de Servicios que se tienen contratados y que son considerados esenciales.

Del mismo modo, se especificarán las interdependencias existentes entre los diferentes activos que soportan o componen la infraestructura crítica. La información anterior deberá ser la suficiente para recoger de manera explícita el alcance de la infraestructura a proteger y con el mismo nivel de detalle que se haya establecido dentro del PSO.

3.3 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores para la infraestructura crítica de que se trate, en el marco del PPE.

El operador crítico deberá hacer referencia dentro de sus diferentes PPE a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

- Con otras infraestructuras críticas del propio operador.
- Con otras infraestructuras estratégicas del propio operador que soportan el servicio esencial.
 - Entre sus propias instalaciones o servicios.
 - Con sus proveedores dentro de la cadena de suministro.
 - Con los proveedores de servicios TIC contratados para esa infraestructura, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.
 - Con los proveedores de servicios de seguridad física, indicando los servicios prestados y el personal y medios empleados.

4. Resultados del Análisis de Riesgos.

El operador crítico deberá reflejar en su PPE los resultados del análisis de riesgos integral realizado sobre la infraestructura crítica. Dicho análisis de riesgos deberá seguir las pautas metodológicas recogidas en su PSO.

A continuación se reflejan los contenidos mínimos relativos al análisis de riesgos realizado que el operador deberá incluir dentro del PPE.

4.1 Amenazas consideradas.

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de las infraestructuras críticas, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

- Las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica.
- Las amenazas que puedan afectar directamente a la infraestructura procedente de las interdependencias identificadas, sean éstas deliberadas o no.
- Las dirigidas al entorno cercano o elementos interdependientes tanto del anteperímetro físico como lógico que puedan afectar a la infraestructura.
- Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.
- Las amenazas que afecten a los sistemas y servicios que soportan la seguridad integral.

4.2 Medidas de seguridad integral existentes.

El operador deberá describir las medidas de seguridad integral (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación) implantadas en la actualidad, con las que se ha contado para la realización del análisis de riesgos. Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales.

Por medidas permanentes se entienden aquellas medidas concretas ya adoptadas por el operador crítico, así como aquellas que considere necesarias instalar en función del resultado del análisis de riesgo realizado respecto de los riesgos, amenazas y consecuencias/impacto sobre sus activos, dirigidas todas ellas a garantizar la seguridad integral de su instalación catalogada como crítica de manera continua.

Por medidas temporales y graduales se entienden aquellas medidas de seguridad de carácter extraordinario que reforzarán a las permanentes y que se deberán implementar de forma ascendente a raíz de la activación de alguno de los niveles de seguridad establecidos respectivamente en el Plan Nacional de Protección de las Infraestructuras Críticas (artículo 16.3 del RD 704/2011), en coordinación con el Plan de Prevención y Protección Antiterrorista, principalmente para los niveles 4 y 5, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta y temporal sobre la instalación por él gestionada.

Dichas medidas deberán permanecer activas durante el tiempo que esté establecido el nivel de alarma, modificándose gradualmente en función de dicho nivel.

Para su mejor comprensión, se recomienda una aproximación por capas para cada nivel, siendo la escala de niveles del 1 al 5 (nivel 1: riesgo bajo; nivel 2: riesgo moderado; nivel 3 riesgo medio; nivel 4: riesgo alto; nivel 5: riesgo muy alto), especificando para cada nivel las medidas de prevención y protección, el tiempo de respuesta y el tiempo de recuperación.

En concreto, el operador deberá describir las medidas concretas de que dispone relativas a:

4.2.1 Organizativas o de Gestión.

El operador deberá indicar si dispone de al menos de las siguientes medidas organizativas o de gestión, y el alcance de cada una de ellas:

- Análisis de Riesgos: Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo.
- Definición de roles y responsabilidades: Asignación de responsabilidades en materia de seguridad.
- Cuerpo normativo definido: Políticas, procedimientos y estándares de seguridad.
- Normas y/o regulaciones de aplicación a la infraestructura crítica, así como identificación de su nivel de cumplimiento.
- Certificación, acreditación y evaluación de seguridad obtenidas para la infraestructura crítica.

4.2.2 Operacionales o Procedimentales.

El operador deberá indicar si dispone de al menos las siguientes medidas operacionales o procedimentales, y el alcance de cada una de ellas.

- Procedimientos para la realización, gestión y mantenimiento de activos críticos (ciclo de vida):

Identificación.
Adquisición.
Catalogación.
Alta.
Actualización.
Baja.

- Procedimientos de formación, concienciación y capacitación (tanto general como específica) para:

Empleados/Operarios.
Personal de seguridad.
Personal contratado.
Etc.

- Procedimientos de Contingencia/Recuperación, en función de los escenarios de contingencia que hayan sido definidos. Se deben detallar además los métodos y políticas de copias de respaldo (backup).

§ 15 Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

• Procedimientos operativos para la monitorización, supervisión y evaluación/auditoría de:

Activos Físicos de la infraestructura (Alcance/Operación/Seguimiento).

Activos Lógicos o de sistemas de operación (Alcance/Operación/Seguimiento).

• Procedimientos de seguridad.

• Procedimientos para la gestión de acceso:

Gestión de usuarios: Altas, bajas y modificaciones, procesos de selección, régimen interno, procedimientos de cese.

Control de accesos temporales:

De personas, vehículos, etc. al recinto general o a recintos restringidos.

Identificadores de usuario temporal de los sistemas (mantenimiento...).

Control de entradas y salidas:

Paquetería, correspondencia, etc.

Soportes, equipos e información (medidas y tecnologías de prevención de fuga de información).

• Procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).

• Procedimientos de gestión y respuesta ante amenazas e incidentes.

• Procedimientos de comunicación e intercambio de información relativos a la protección de infraestructuras críticas (a través del protocolo de incidentes proporcionado por el CNPIC al efecto):

Con el CNPIC:

Sobre incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de la infraestructura.

Sobre variación de datos sobre la organización y medidas de seguridad, datos de descripción de la infraestructura, etc.

Con el CERTSI:

A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes de la infraestructura y la disponibilidad de los servicios por ella prestada.

4.2.3 De Protección o Técnicas.

• Medidas de Prevención y Detección:

Medidas y elementos de seguridad física y electrónica para la protección del perímetro y control de accesos:

Vallas, zonas de seguridad, detectores de intrusos, cámaras de video vigilancia/CCTV, puertas y esclusas, cerraduras, lectores de matrículas, arcos de seguridad, tornos, scanners, tarjetas activas, lectores de tarjetas, etc.

Medidas y elementos de ciberseguridad:

• Firewalls, DMZ, IPSs, IDSs, segmentación y aislamiento de redes, cifrado, VPNs, elementos y medidas de control de acceso de usuarios (tokens, controles biométricos, etc.), medidas de instalación y configuración segura de elementos técnicos, correladores de eventos y logs, protección frente Malware, etc.

Redundancia de sistemas (hardware y software).

Otros.

• Medidas de Coordinación y Monitorización:

Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.).

Equipos de vigilancia (turnos, rondas, volumen, etc.).

Sistemas de comunicación.

Otros.

4.3 Valoración de riesgos.

En este apartado se describirán las principales conclusiones obtenidas en el análisis de riesgos. Para cada par activo/amenaza se deberá especificar la valoración efectuada, sobre la base de los criterios especificados en la metodología de análisis de riesgos detallada en el PSO. Dentro de este apartado deberá incluirse, para cada par activo/amenaza, la siguiente información:

- Quién ha evaluado/aprobado el riesgo y la estrategia de tratamiento asociada.
- Criterios de valoración de riesgos adoptados.
- Fecha del último análisis llevado a cabo.
- Resultado/conclusión sobre el nivel de riesgo soportado.
- Evolución en el tiempo de la evaluación del par activo/amenaza

En particular, deberán detallarse los riesgos asumidos en activos con niveles de impacto elevado y baja probabilidad de ocurrencia, que deberán ser validados por el CNPIC.

5. Plan de acción propuesto (por activo).

En caso de ser pertinente y preverse la disposición de medidas complementarias a las existentes a implementar en los próximos tres años, se deberá describir, como parte integrante del PPE:

- Listado de las medidas complementarias a disponer (físicas o de ciberseguridad).
- Una explicación de la operativa resultante para cada tipo de protección (físico y lógico).

El operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos. En concreto, deberá incluir la siguiente información:

- Activo de aplicación.
- Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
- Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
- Carácter de la medida, permanente, temporal o gradual.

6. Documentación complementaria.

El operador crítico incorporará como anexo la planimetría general de la instalación o sistema y de sus sistemas de información, así como aquellos otros planos que incorporen la ubicación de las medidas de seguridad implementadas. A su vez, se podrá adjuntar aquella otra información que se pueda generar de los diferentes apartados de este documento.

Se hará una breve referencia a todos aquellos planes de diferente tipo (emergencia, autoprotección, ciberseguridad, etc.), que afecten a la instalación o sistema con el fin de establecer una adecuada coordinación entre ellos, así como toda aquella normativa y buenas prácticas que regulen el buen funcionamiento del servicio esencial prestado por esa infraestructura y los motivos por los cuales le son de aplicación.

La normativa a incluir comprenderá la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

- Seguridad Física.
- Ciberseguridad.
- Seguridad de la Información.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

§ 16

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

Jefatura del Estado
«BOE» núm. 102, de 29 de abril de 2011
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2011-7630

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

En esa línea, se han emprendido diversas actuaciones a nivel nacional, como la aprobación, por la Secretaría de Estado de Seguridad del Ministerio del Interior, de un primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas. Así mismo, con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas, mediante el cual se dio un impulso decisivo en dicha materia. El desarrollo y aplicación de este Acuerdo supone un avance cualitativo de primer orden para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales.

Paralelamente, existen también una serie de actuaciones desarrolladas a nivel internacional en el ámbito europeo: tras los terribles atentados de Madrid, el Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004 la Comisión adoptó una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa europeo de protección de infraestructuras críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network-CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las Comunidades Autónomas.

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente

una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

La Ley consta de 18 artículos, estructurados en 3 Títulos. El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece, finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Asimismo, la Ley consta de cuatro Disposiciones Adicionales y cinco Disposiciones Finales.

Si bien el contenido material de la Ley es eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos que integran el Sistema de Protección de Infraestructuras Críticas, así como en todo lo relativo a los diferentes planes de protección, se ha optado por dotar a esta norma de rango legal, de acuerdo con el criterio del Consejo de Estado, a fin de poder cubrir suficientemente aquellas obligaciones que la Ley impone y que requieren de una cobertura legal específica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

2. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas, según lo dispuesto en los párrafos e) y f) del artículo 2 de la misma.

Artículo 2. *Definiciones.*

A los efectos de la presente Ley, se entenderá por:

a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

f) Infraestructuras críticas europeas: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE).

g) Zona crítica: aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.

h) Criterios horizontales de criticidad: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

i) Análisis de riesgos: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

j) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

k) Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

l) Información sensible sobre protección de infraestructuras estratégicas: los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

m) Operadores críticos: las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley.

n) Nivel de Seguridad: aquel cuya activación por el Ministerio del Interior está previsto en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

o) Catálogo Nacional de Infraestructuras Estratégicas: la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

Artículo 3. *Ámbito de aplicación.*

1. La presente Ley se aplicará a las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.

2. Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se registrarán, a efectos de control administrativo, por su propia normativa y procedimientos.

3. La aplicación de esta Ley se efectuará sin perjuicio de:

a) La misión y funciones del Centro Nacional de Inteligencia establecidas en su normativa específica, contando siempre con la necesaria colaboración y complementariedad con aquéllas.

b) Los criterios y disposiciones contenidos en la Ley 25/1964, de 29 de abril, sobre energía nuclear, y normas de desarrollo de la misma, y en la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear, reformada por la Ley 33/2007, de 7 de noviembre.

c) Lo previsto en el Programa Nacional de Seguridad de la Aviación Civil contemplado en la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y su normativa complementaria.

Artículo 4. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será el responsable del Catálogo Nacional de Infraestructuras Estratégicas (en adelante, el Catálogo), instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley.

2. La competencia para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas, corresponderá al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, incluidas las propuestas, en su caso, del órgano competente de las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público en relación con las infraestructuras ubicadas en su demarcación territorial.

TÍTULO II

El Sistema de Protección de Infraestructuras Críticas

Artículo 5. *Finalidad.*

1. El Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.

2. Son agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes:

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.

b) El Centro Nacional para la Protección de las Infraestructuras Críticas.

c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.

d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

- e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
- f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.
- g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- i) Los operadores críticos del sector público y privado.

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales.

Para el desempeño de su cometido, el Reglamento de desarrollo de esta Ley determinará sus competencias en la materia, que ejercerá con la asistencia de los demás integrantes del Sistema y, principalmente, del Centro Nacional para la Protección de las Infraestructuras Críticas.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, el CNPIC) como órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

2. El CNPIC dependerá orgánicamente de la Secretaría de Estado de Seguridad, y sus funciones serán las que reglamentariamente se establezcan.

3. Sin perjuicio de lo dispuesto en el apartado anterior, corresponderá al CNPIC la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.

Artículo 8. *Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

1. Por cada sector estratégico, se designará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema. El nombramiento, alta o baja en éste de un ministerio u organismo con responsabilidad sobre un sector estratégico se efectuará mediante la modificación del anexo de la presente Ley.

2. Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia. Para ello, colaborarán con el Ministerio del Interior a través de la Secretaría de Estado de Seguridad.

3. Con tales objetivos, los ministerios y organismos del Sistema desempeñarán las funciones que reglamentariamente se determinen.

4. Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo de la presente Ley.

Artículo 9. *Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

1. Los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, una serie de facultades respecto de las infraestructuras críticas localizadas en su demarcación.

2. El desarrollo reglamentario de dichas facultades en todo caso incluirá la intervención, a través de las Fuerzas y Cuerpos de Seguridad, en la implantación de los diferentes Planes de Protección Específico y de Apoyo Operativo, así como la propuesta a la Secretaría de Estado de Seguridad de la declaración de una zona como crítica.

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

3. No obstante lo dispuesto en el apartado primero de este artículo, las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, aquellas facultades de las Delegaciones del Gobierno relativas a la coordinación de los cuerpos policiales autonómicos y, en su caso, a la activación por aquellos del Plan de Apoyo Operativo que corresponda para responder ante una alerta de seguridad.

Artículo 10. *Comunidades Autónomas y Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

2. En todo caso, las Comunidades Autónomas mencionadas en el apartado anterior participarán en el proceso de declaración de una zona como crítica, en la aprobación del Plan de Apoyo Operativo que corresponda, y en las reuniones del Grupo de Trabajo Interdepartamental. Asimismo, serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas.

3. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

Artículo 11. *Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad.

2. La Comisión será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas.

3. Sus funciones y composición serán las que reglamentariamente se establezcan.

Artículo 12. *Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Sistema contará con un Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo), cuya composición y funciones se determinarán reglamentariamente.

2. Le corresponderá, en todo caso, la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

Artículo 13. *Operadores críticos.*

1. Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.

b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

h) Constituir un Área de Seguridad del Operador, de la manera que reglamentariamente se determine

2. Será requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.

3. La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan.

4. Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

TÍTULO III

Instrumentos y comunicación del Sistema

Artículo 14. *Instrumentos de planificación del Sistema.*

1. La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes planes de actuación:

- a) El Plan Nacional de Protección de las Infraestructuras Críticas.
- b) Los Planes Estratégicos Sectoriales.
- c) Los Planes de Seguridad del Operador.
- d) Los Planes de Protección Específicos.
- e) Los Planes de Apoyo Operativo.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, elaborará el Plan Nacional de Protección de las Infraestructuras Críticas, siendo éste el documento estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha contra el terrorismo.

3. Los Planes Estratégicos Sectoriales serán asimismo elaborados por el Grupo de Trabajo y aprobados por la Comisión, e incluirán, por sectores, los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo.

4. Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

5. Los Planes de Apoyo Operativo deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos.

6. El contenido concreto y el procedimiento de elaboración, aprobación y registro de cada uno de los planes serán los que se determinen reglamentariamente.

Artículo 15. *Seguridad de las comunicaciones.*

1. La Secretaría de Estado de Seguridad arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC, así como su difusión a los organismos autorizados.

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

Artículo 16. *El Responsable de Seguridad y Enlace.*

1. Los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca.

2. En todo caso, el Responsable de Seguridad y Enlace designado deberá contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica.

3. Las funciones específicas del Responsable de Seguridad y Enlace serán las previstas reglamentariamente.

Artículo 17. *El Delegado de Seguridad de la Infraestructura Crítica.*

1. Los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un Delegado de Seguridad para dicha infraestructura.

2. El plazo para efectuar dicha comunicación, así como las funciones específicas del Delegado de Seguridad de la Infraestructura Crítica, serán los que reglamentariamente se establezcan.

Artículo 18. *Seguridad de los datos clasificados.*

El operador crítico deberá garantizar la seguridad de los datos clasificados relativos a sus propias infraestructuras, mediante los medios de protección y los sistemas de información adecuados que reglamentariamente se determinen.

Disposición adicional primera. *Normativa y régimen económico aplicable a la Comisión Nacional para la Protección de las Infraestructuras Críticas y al Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

En lo no previsto en la presente Ley, se estará a lo dispuesto para el funcionamiento de los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo

§ 16 Ley que establece medidas para la protección de las infraestructuras críticas

Común. Así mismo, el funcionamiento y los trabajos de la Comisión, así como del Grupo de Trabajo previstos en la presente norma se llevarán a cabo con cargo a las dotaciones presupuestarias y los medios personales y tecnológicos del Ministerio del Interior, sin que supongan incremento alguno del gasto público.

Disposición adicional segunda. *Clasificación de los Planes.*

Los Planes a los que se refiere el artículo 14 de la presente Ley tendrán la clasificación que les corresponda en virtud de la normativa vigente en la materia, la cual deberá constar de forma expresa en el instrumento de su aprobación.

Disposición adicional tercera. *Fuerzas y Cuerpos de Seguridad.*

Las referencias efectuadas en la presente Ley a las Fuerzas y Cuerpos de Seguridad incluyen, en todo caso, a los Cuerpos policiales dependientes de las Comunidades Autónomas con competencias estatutarias reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

Disposición adicional cuarta. *Ceuta y Melilla.*

De conformidad con lo establecido en los Estatutos de Autonomía de las Ciudades de Ceuta y Melilla, los Consejos de Gobierno de ambas, de acuerdo con la Delegación del Gobierno respectiva, podrán emitir informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras situadas en ellas que sean objeto de la presente Ley.

Disposición final primera. *Título competencial.*

Esta Ley se dicta al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29.^a de la Constitución Española en materia de seguridad pública.

Disposición final segunda. *Competencias en materia de Protección Civil.*

Lo dispuesto en esta Ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía.

Disposición final tercera. *Incorporación de Derecho comunitario.*

Mediante esta Ley y sus ulteriores desarrollos reglamentarios se incorpora al Derecho español la Directiva 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

1. Se habilita al Gobierno para que en plazo de seis meses dicte el Reglamento de la presente Ley.

2. Igualmente se habilita al Gobierno a modificar por Real Decreto, a propuesta del titular del Ministerio del Interior y del titular del Departamento competente por razón de la materia, el Anexo de esta Ley.

3. En el ámbito de sus competencias, las Comunidades Autónomas podrán igualmente elaborar las normas reglamentarias necesarias para el desarrollo de la presente Ley.

Disposición final quinta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Sectores estratégicos y Ministerios/Organismos del sistema competentes

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia.
	Ministerio Interior.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio. Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación.
	Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino.
Energía.	Ministerio Sanidad, Política Social e Igualdad.
Salud.	Ministerio Industria, Turismo y Comercio.
	Ministerio Sanidad, Política Social e Igualdad.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Ciencia e Innovación.
	Ministerio Industria, Turismo y Comercio.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Ciencia e Innovación.
Transporte.	Ministerio Política Territorial y Administración Pública.
	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

§ 17

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas

Ministerio del Interior
«BOE» núm. 121, de 21 de mayo de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-8849

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas habilita al Gobierno, en su disposición final cuarta, para dictar el Reglamento de ejecución de desarrollo de la mencionada Ley.

En cumplimiento de este mandato, el presente real decreto se aprueba, en primer lugar, con la finalidad de desarrollar, concretar y ampliar los aspectos contemplados en la citada Ley, máxime cuando del tenor de la misma se desprende no sólo la articulación de un complejo Sistema de carácter interdepartamental para la protección de las infraestructuras críticas, compuesto por órganos y entidades tanto de las Administraciones Públicas como del sector privado, sino el diseño de todo un planeamiento orientado a prevenir y proteger las denominadas infraestructuras críticas de las amenazas o actos intencionados provenientes de figuras delictivas como el terrorismo, potenciados a través de las tecnologías de la comunicación.

En segundo lugar, este texto normativo no sólo es coherente con el marco legal del que trae causa, sino que además sirve a los fines del Sistema Nacional de Gestión de Situaciones de Crisis y cumple con la transposición obligatoria de la Directiva 2008/114/CE, del Consejo de la Unión Europea, de 8 de diciembre, en vigor desde el 12 de enero de 2009, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. A ello obedecen las amplias previsiones que el texto contempla en el ámbito de los diferentes Planes que deben elaborar tanto las Administraciones Públicas –en el caso del Plan Nacional de Protección de las Infraestructuras Críticas, los Planes Estratégicos Sectoriales y los Planes de Apoyo Operativo– como las empresas, organizaciones o instituciones clasificadas como operadores críticos, a quienes la Ley asigna una serie de obligaciones, entre las que se encuentran la elaboración de sendos instrumentos de planificación: los Planes de Seguridad del Operador y los Planes de Protección Específicos.

Asimismo, la Ley prevé que los operadores críticos designen a un Responsable de Seguridad y Enlace –a quien se exige la habilitación de director de seguridad que concede el Ministerio del Interior al personal de seguridad de las empresas de Seguridad Privada en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, o habilitación equivalente, según su normativa específica–. Igualmente, se contempla la designación de un Delegado de Seguridad por cada una de las infraestructuras críticas identificadas.

En lo que a su contenido se refiere, el presente real decreto consta de un artículo único, una disposición transitoria única y dos disposiciones finales. Por su parte, el Reglamento consta de 36 artículos estructurados en cuatro Títulos. El Título I contiene las cuestiones generales relativas a su objeto y ámbito de aplicación, y dedica un artículo a la figura del Catálogo Nacional de Infraestructuras Estratégicas, como instrumento de la Secretaría de Estado de Seguridad del Ministerio del Interior que debe aglutinar todos los datos y la valoración de la criticidad de las citadas infraestructuras y que será empleado como base para planificar las actuaciones necesarias en materia de seguridad y protección de las mismas, al nutrirse de las aportaciones de los propios operadores. El Título II está plenamente dedicado al Sistema de Protección de Infraestructuras Críticas, y desarrolla, entre otras, las previsiones legales relativas a los órganos creados por la Ley, esto es, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), la Comisión Nacional para la Protección de las Infraestructuras Críticas y el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, concretando la composición, competencias y funcionamiento de todos ellos. El Título III se encarga de la regulación de los instrumentos de planificación, centrándose en cada uno de los Planes antes citados, cuyo proceso de elaboración, aprobación y registro, así como sus contenidos materiales, regula con mayor detalle. Finalmente, el Título IV está consagrado a la seguridad de las comunicaciones y a las figuras del Responsable de Seguridad y Enlace y del Delegado de Seguridad de la infraestructura crítica.

La tramitación del presente real decreto ha sido fruto de un intenso diálogo y colaboración entre los distintos Departamentos Ministeriales y organismos afectados, contando también con la aportación de las distintas Comunidades Autónomas y del sector empresarial, tras el trámite de información pública otorgado a todos ellos, lo que ha contribuido a dotar al texto de un extenso y, por otro lado, imprescindible, grado de consenso.

En su virtud, a propuesta del Vicepresidente Primero del Gobierno y Ministro del Interior, con la aprobación previa del Vicepresidente Tercero del Gobierno y Ministro de Política Territorial y Administración Pública, con el informe favorable de la Vicepresidenta Segunda del Gobierno y Ministra de Economía y Hacienda, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 20 de mayo de 2011,

DISPONGO:

TÍTULO I

Artículo único. *Aprobación del Reglamento de Protección de las infraestructuras críticas.*

En desarrollo y ejecución de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, se aprueba el Reglamento de Protección de las Infraestructuras Críticas, cuyo texto se inserta a continuación.

Disposición transitoria única. *Unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General.*

Las unidades y puestos de trabajo con nivel orgánico inferior a Subdirección General del Centro Nacional para la Protección de las Infraestructuras Críticas continuarán subsistentes y serán retribuidos con cargo a los mismos créditos presupuestarios, hasta que se aprueben las relaciones de puestos de trabajo adaptadas a la estructura organizativa proyectada en el ámbito de la protección de las infraestructuras críticas. Dicha adaptación en ningún caso podrá generar incremento de gasto público.

Disposición final primera. *Título competencial.*

Este real decreto se dicta al amparo de la competencia atribuida al Estado en materia de seguridad pública en el artículo 149.1.29.^a de la Constitución.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

TÍTULO I

Disposiciones generales

CAPÍTULO I

Objeto y ámbito de aplicación

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto desarrollar el marco previsto en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, a fin de concretar las actuaciones de los distintos órganos integrantes del Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) así como los diferentes instrumentos de planificación del mismo.

2. Asimismo, regula las especiales obligaciones que deben asumir tanto el Estado como los operadores de aquellas infraestructuras que se determinen como críticas, según lo dispuesto en el artículo 2, párrafos e) y f) de la citada Ley.

Artículo 2. *Ámbito de aplicación.*

El ámbito de aplicación del presente reglamento será el previsto por el artículo 3 de la Ley 8/2011, de 28 de abril.

CAPÍTULO II

El Catálogo Nacional de Infraestructuras Estratégicas

Artículo 3. *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Catálogo Nacional de infraestructuras estratégicas (en adelante, el Catálogo) es el registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas así como aquellas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE.

2. La finalidad principal del Catálogo es valorar y gestionar los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquéllas y, en caso de ser necesario, activar, conforme a lo previsto por el Plan Nacional de Protección de las Infraestructuras Críticas, una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate.

Artículo 4. *Contenido del Catálogo.*

1. En el Catálogo deberán incorporarse, entre otros datos, los relativos a la descripción de las infraestructuras, su ubicación, titularidad y administración, servicios que prestan, medios de contacto, nivel de seguridad que precisan en función de los riesgos evaluados así como la información obtenida de las Fuerzas y Cuerpos de Seguridad.

2. El Catálogo se nutrirá de la información que le faciliten al Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, CNPIC) los operadores de las infraestructuras así como el resto de sujetos responsables del Sistema relacionados en el artículo 5 de la Ley 8/2011, de 28 de abril.

3. El Catálogo Nacional de Infraestructuras Estratégicas tiene, conforme a lo dispuesto en la legislación vigente en materia de secretos oficiales, la calificación de SECRETO, conferida por Acuerdo de Consejo de Ministros de 2 de noviembre de 2007, calificación que comprende, además de los datos contenidos en el propio Catálogo, los equipos, aplicaciones informáticas y sistemas de comunicaciones inherentes al mismo, así como el nivel de habilitación de las personas que pueden acceder a la información en él contenida.

Artículo 5. *Gestión y actualización del Catálogo.*

1. La custodia, gestión y mantenimiento del Catálogo Nacional de infraestructuras estratégicas corresponde al Ministerio del Interior, a través de la Secretaría de Estado de Seguridad.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será responsable de clasificar una infraestructura como estratégica y, en su caso, como infraestructura crítica o infraestructura crítica europea, así como de incluirla por vez primera en el Catálogo, previa comprobación de que cumple uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) de la Ley 8/2011, de 28 de abril.

3. El proceso de identificación de una infraestructura como crítica se realizará por el CNPIC, que podrá recabar la participación y el asesoramiento del interesado, así como de los agentes del Sistema competentes, a los que informará posteriormente del resultado de tal proceso.

4. La clasificación de una infraestructura como crítica europea supondrá la obligación adicional de comunicar su identidad a otros Estados miembros que puedan verse afectados de forma significativa por aquella, de acuerdo con lo previsto por la Directiva 2008/114/CE. En tal caso, las notificaciones, en reciprocidad con otros Estados miembros, se realizarán por el CNPIC, de acuerdo con la clasificación de seguridad que corresponda según la normativa vigente.

5. En los casos en que se produzca una modificación relevante que afecte a las infraestructuras inscritas y que sea de interés a los efectos previstos en el presente reglamento, los operadores críticos responsables de las mismas facilitarán, a través de los medios puestos a su disposición por el Ministerio del Interior, los nuevos datos de aquéllas al CNPIC, que deberá validarlos con carácter previo a su incorporación al Catálogo. En todo caso, la actualización de los datos disponibles deberá hacerse con periodicidad anual.

TÍTULO II

Los agentes del Sistema de Protección de Infraestructuras Críticas

Artículo 6. *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las Infraestructuras Críticas Nacionales, para lo cual su titular, u órgano en quien delegue, ejercerá las siguientes funciones:

a) Diseñar y dirigir la estrategia nacional de protección de infraestructuras críticas.

b) Aprobar el Plan Nacional de Protección de las Infraestructuras Críticas y dirigir su aplicación, declarando en su caso los niveles de seguridad a establecer en cada momento, conforme al contenido de dicho Plan y en coordinación con el Plan de Prevención y Protección Antiterrorista.

c) Aprobar los Planes de Seguridad de los Operadores y sus actualizaciones a propuesta del CNPIC, tomando en su caso, como referencia, las actuaciones del órgano u organismo competente para otorgar a aquéllos las autorizaciones correspondientes en virtud de su normativa sectorial.

d) Aprobar los diferentes Planes de Protección Específicos o las eventuales propuestas de mejora de éstos a propuesta del CNPIC, en los términos de lo dispuesto en el artículo 26 de este reglamento.

e) Aprobar los Planes de Apoyo Operativo, así como supervisar y coordinar la implantación de los mismos y de aquellas otras medidas de prevención y protección que

deban activarse tanto por las Fuerzas y Cuerpos de Seguridad y por las Fuerzas Armadas, en su caso, como por los propios responsables de seguridad de los operadores críticos.

f) Aprobar, previo informe del CNPIC, la declaración de una zona como crítica, a propuesta de las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

g) Identificar los diferentes ámbitos de responsabilidad en la protección de infraestructuras críticas; analizando los mecanismos de prevención y respuesta previstos por cada uno de los actores implicados.

h) Emitir las instrucciones y protocolos de colaboración dirigidos tanto al personal y órganos ajenos al Ministerio del Interior como a los operadores de las infraestructuras estratégicas, así como fomentar la adopción de buenas prácticas.

i) Responder del cumplimiento de las obligaciones y compromisos asumidos por España en el marco de la Directiva 2008/114/CE, sin perjuicio de las competencias que corresponden al Ministerio de Asuntos Exteriores y de Cooperación.

j) Supervisar, dentro del ámbito de aplicación de este reglamento, los proyectos y estudios de interés y coordinar la participación en programas financieros y subvenciones procedentes de la Unión Europea.

k) Colaborar con los Ministerios y organismos integrados en el Sistema en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril y del presente reglamento.

l) Cualesquiera otras funciones que, eventualmente, pudieran acordarse por la Comisión Delegada del Gobierno para Situaciones de Crisis.

Artículo 7. *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

El CNPIC del Ministerio del Interior, orgánicamente dependiente de la Secretaría de Estado de Seguridad, tendrá el nivel orgánico que se determine en la correspondiente relación de puestos de trabajo, y desempeñará las siguientes funciones:

a) Asistir al Secretario de Estado de Seguridad en la ejecución de sus funciones en materia de protección de infraestructuras críticas, actuando como órgano de contacto y coordinación con los agentes del Sistema.

b) Ejecutar y mantener actualizado el Plan Nacional de Protección de las Infraestructuras Críticas conforme a lo previsto en el artículo 16 de este reglamento.

c) Determinar la criticidad de las infraestructuras estratégicas incluidas en el Catálogo.

d) Mantener operativo y actualizado el Catálogo, estableciendo los procedimientos de alta, baja y modificación de las infraestructuras, tanto nacionales como europeas, que en él se incluyan en virtud de los criterios horizontales y de los efectos de interdependencias sectoriales a partir de la información que le suministren los operadores y el resto de agentes del Sistema, así como establecer su clasificación interna.

e) Llevar a cabo las siguientes funciones respecto a los instrumentos de planificación previstos en este reglamento:

Dirigir y coordinar los análisis de riesgos que se realicen por los organismos especializados, públicos o privados, sobre cada uno de los sectores estratégicos en el marco de los Planes Estratégicos Sectoriales, para su estudio y deliberación por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Establecer los contenidos mínimos de los Planes de Seguridad de los Operadores, de los Planes de Protección Específicos y de los Planes de Apoyo Operativo y supervisar el proceso de elaboración de éstos, recomendando, en su caso, el orden de preferencia de las contramedidas y los procedimientos a adoptar para garantizar su protección ante ataques deliberados.

Evaluar, tras la emisión de los correspondientes informes técnicos especializados, los Planes de Seguridad del Operador y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Analizar los Planes de Protección Específicos facilitados por los operadores críticos respecto a las diferentes infraestructuras críticas o infraestructuras críticas europeas de su

titularidad y proponerlos, en su caso, para su aprobación, al Secretario de Estado de Seguridad, u órgano en quien delegue.

Validar los Planes de Apoyo Operativo diseñados para cada una de las infraestructuras críticas existentes en el territorio nacional por el Cuerpo Policial estatal o, en su caso, autonómico competente, previo informe, respectivamente, de las Delegaciones del Gobierno en las Comunidades Autónomas o de las Comunidades Autónomas que tengan competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

f) Elevar al Secretario de Estado de Seguridad, u órgano en quien delegue, las propuestas para la declaración de una zona como crítica que se efectúen.

g) Implantar, bajo el principio general de confidencialidad, mecanismos permanentes de información, alerta y comunicación con todos los agentes del Sistema.

h) Recopilar, analizar, integrar y valorar la información sobre infraestructuras estratégicas procedente de instituciones públicas, servicios policiales, operadores y de los diversos instrumentos de cooperación internacional para su remisión al Centro Nacional de Coordinación Antiterrorista del Ministerio del Interior o a otros organismos autorizados.

i) Participar en la realización de ejercicios y simulacros en el ámbito de la protección de las infraestructuras críticas.

j) Coordinar los trabajos y la participación de expertos en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas, en los ámbitos nacional e internacional.

k) Ser, en el ámbito de la Protección de las Infraestructuras Críticas, el Punto Nacional de Contacto con organismos internacionales y con la Comisión Europea, así como elevar a ésta, previa consulta al Centro Nacional de Coordinación Antiterrorista, los informes sobre evaluación de amenazas y tipos de vulnerabilidades y riesgos encontrados en cada uno de los sectores en los que se hayan designado infraestructuras críticas europeas, en los plazos y condiciones marcados por la Directiva.

l) Ejecutar las acciones derivadas del cumplimiento de la Directiva 2008/114/CE en representación de la Secretaría de Estado de Seguridad.

Artículo 8. *Los Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

Los ministerios y organismos del Sistema a los que se refiere el artículo 8 de la Ley 8/2011, de 28 de abril tendrán las siguientes competencias:

a) Participar, a través del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas, con el apoyo, en su caso, de los operadores, en la elaboración de los Planes Estratégicos Sectoriales, así como proceder a su revisión y actualización en los términos previstos en este reglamento.

b) Verificar, en el ámbito de sus competencias, el cumplimiento de los Planes Estratégicos Sectoriales y de las actuaciones derivadas de éstos, con excepción de las que se correspondan con medidas de seguridad concretas establecidas en infraestructuras específicas, o las que deban ser realizadas por otros órganos de la Administración General del Estado, conforme a su legislación específica.

c) Colaborar con la Secretaría de Estado de Seguridad tanto en la designación de los operadores críticos como en la elaboración de toda norma sectorial que se dicte en desarrollo de la Ley 8/2011, de 28 de abril, así como del presente reglamento.

d) Proporcionar asesoramiento técnico a la Secretaría de Estado de Seguridad en la catalogación de las infraestructuras dentro de su sector de competencia, poniendo a disposición del CNPIC en su caso la información técnica que ayude a determinar su criticidad, para su inclusión, exclusión o modificación en el Catálogo.

e) Custodiar, en los términos de la normativa sobre materias clasificadas y secretos oficiales, la información sensible sobre protección de infraestructuras estratégicas de la que dispongan en calidad de agentes del Sistema.

f) Designar a una persona para participar en los Grupos de Trabajo Sectoriales que, eventualmente, puedan crearse en el ámbito de la protección de infraestructuras críticas.

g) Participar, a solicitud del CNPIC o por iniciativa propia, en los diferentes grupos de trabajo y reuniones sobre protección de infraestructuras críticas relacionadas con su sector de coordinación, en los ámbitos nacional e internacional.

h) Colaborar con la Secretaría de Estado de Seguridad en las acciones derivadas del cumplimiento de la Directiva 2008/114/CE, conforme a lo dispuesto en el artículo 7, apartado l), de este reglamento.

i) Participar en el proceso de clasificación de una infraestructura como crítica, incluyendo el ejercicio de la facultad de propuesta a tal fin.

Artículo 9. *Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

Bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, respecto de las infraestructuras críticas localizadas en su territorio, las siguientes facultades:

a) Coordinar la actuación de las Fuerzas y Cuerpos de Seguridad del Estado ante una alerta de seguridad, y velar por la aplicación del Plan Nacional de Protección de Infraestructuras Críticas en caso de activación de éste.

b) Colaborar, en función de su ámbito territorial de actuación, con otros órganos de la Administración u organismos públicos competentes conforme a su legislación específica, así como con las delegaciones territoriales de otros ministerios y organismos del Sistema en las acciones que se desarrollen para el cumplimiento de los Planes Sectoriales vigentes en materia de protección de infraestructuras críticas.

c) Participar en la implantación de los diferentes Planes de Protección Específicos en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, en los términos en los que se expresa el Capítulo IV del Título III de este reglamento.

d) Intervenir, a través del Cuerpo Policial estatal competente, y en colaboración con el responsable de seguridad de la infraestructura, en la implantación de los diferentes Planes de Apoyo Operativo en aquellas infraestructuras críticas o infraestructuras críticas europeas existentes en su territorio, conforme a lo establecido en el Capítulo V del Título III de este reglamento.

e) Proponer a la Secretaría de Estado de Seguridad a través del CNPIC la declaración de zona crítica sobre la base de la existencia de varias infraestructuras críticas o infraestructuras críticas europeas en una zona geográfica continua, con el fin de lograr una protección coordinada entre los diferentes operadores titulares y las Fuerzas y Cuerpos de Seguridad.

f) Custodiar la información sensible sobre protección de infraestructuras estratégicas de que dispongan en calidad de agentes del Sistema, en aplicación de la normativa vigente sobre materias clasificadas y secretos oficiales.

Artículo 10. *Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, las facultades previstas en los párrafos c), d), e) y f) del artículo anterior dada la existencia en ellas de Cuerpos policiales autonómicos, y sin perjuicio de que las respectivas Delegaciones del Gobierno en dichas Comunidades Autónomas tengan conocimiento de la información sensible y de los planes a que se refiere el presente reglamento.

2. En todo caso, la coordinación de las actuaciones que se lleven a cabo en materia de protección de las infraestructuras críticas entre las Fuerzas y Cuerpos de Seguridad del Estado y los Cuerpos policiales de las Comunidades Autónomas con competencias en materia de seguridad, se regirá por lo estipulado en los acuerdos de las Juntas de Seguridad correspondientes.

3. Las Comunidades Autónomas no incluidas en el apartado primero del presente artículo participarán en el Sistema y en los órganos colegiados del mismo de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

4. De acuerdo con lo dispuesto en sus Estatutos de Autonomía, las Ciudades de Ceuta y Melilla, a través de sus Consejos de Gobierno y de acuerdo con la Delegación de Gobierno respectiva, podrán emitir los oportunos informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras críticas y críticas europeas situadas en su territorio.

Artículo 11. *La Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. La Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) desempeñará las siguientes funciones:

a) Preservar, garantizar y promover la existencia de una cultura de seguridad de las infraestructuras críticas en el ámbito de las Administraciones públicas.

b) Promover la aplicación efectiva de las disposiciones de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas por parte de todos los sujetos responsables del sistema de protección de infraestructuras críticas, a partir de los informes emitidos al respecto por parte del Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

c) Llevar a cabo las siguientes actuaciones a propuesta del Grupo de Trabajo:

Aprobar los Planes Estratégicos Sectoriales.

Designar a los operadores críticos.

Aprobar la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, estableciendo sus objetivos y sus marcos de actuación.

d) Impulsar aquéllas otras tareas que se estimen precisas en el marco de la cooperación interministerial para la protección de las infraestructuras críticas.

2. La Comisión será presidida por el Secretario de Estado de Seguridad, y sus miembros serán:

a) En representación del Ministerio del Interior:

El Director General de la Policía y de la Guardia Civil.

El Director General de Protección Civil y Emergencias.

El Director del CNPIC, que ejercerá las funciones de Secretario de la Comisión.

b) En representación del Ministerio de Defensa, el Director General de Política de Defensa.

c) En representación del Centro Nacional de Inteligencia, un Director General designado por el Secretario de Estado-Director de aquél.

d) En representación del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, su Director.

e) En representación del Consejo de Seguridad Nuclear, el Director Técnico de Protección Radiológica.

f) En representación de cada uno de los ministerios integrados en el Sistema, una persona con rango igual o superior a Director General, designada por el titular del Departamento ministerial correspondiente en razón del sector de actividad material que corresponda.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones de la Comisión un representante con voz y voto por cada una de las Comunidades Autónomas que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público. También participará, igualmente con voz y voto, un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

En su caso, y cuando su presencia y criterio resulte imprescindible por razón de los temas a tratar, podrán ser convocados, por decisión de su presidente, organismos, expertos u otras Administraciones públicas.

4. La Comisión se reunirá al menos una vez al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno previa convocatoria de su Presidente, quien determinará el orden del día de la reunión en los términos previstos para los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La secretaría de la Comisión radicará en el Director del CNPIC.

5. La Comisión será asistida por el Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

Artículo 12. *El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo) desempeña las siguientes funciones:

a) Elaborar, con la colaboración de los agentes del Sistema afectados y el asesoramiento técnico pertinente, los diferentes Planes Estratégicos Sectoriales para su presentación a la Comisión, conforme a lo previsto en el Título III, Capítulo II, de este reglamento.

b) Proponer a la Comisión la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

c) Proponer a la Comisión la creación, modificación o supresión de grupos de trabajo sectoriales o de carácter técnico, supervisando, coordinando y efectuando el seguimiento de los mismos y de sus trabajos e informando oportunamente de los resultados obtenidos a la Comisión.

d) Efectuar los estudios y trabajos que, en el marco de este reglamento, le encomiende la Comisión. Para ello podrá contar, si es necesario, con el apoyo de personal técnico especializado.

2. El Grupo de Trabajo estará presidido por el Director del CNPIC, y estará compuesto por:

a) Un representante de cada uno de los ministerios del Sistema, designados por el titular del departamento ministerial correspondiente.

b) Un representante de la Dirección Adjunta Operativa del Cuerpo Nacional de Policía, designado por el titular de ésta.

c) Un representante de la Dirección Adjunta Operativa de la Guardia Civil, designado por el titular de aquélla.

d) Un representante de la Dirección General de Protección Civil y Emergencias del Ministerio del Interior, designado por el titular de ésta.

e) Un representante del Estado Mayor Conjunto de la Defensa, designado por el Jefe del Estado Mayor de la Defensa.

f) Un representante del Centro Nacional de Inteligencia, designado por el Secretario de Estado Director de dicho Centro.

g) Un representante del Departamento de Infraestructura y Seguimiento para Situaciones de Crisis, designado por el titular del Ministerio de la Presidencia u órgano en quien delegue, a propuesta del Director del Gabinete de la Presidencia del Gobierno.

h) Un representante del Consejo de Seguridad Nuclear, designado por el Presidente de dicho organismo.

i) Un representante del CNPIC, con funciones de Secretario.

3. Además de los miembros mencionados en el apartado anterior, asistirá a las reuniones del Grupo de Trabajo un representante, con voz y voto por cada una de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y para el mantenimiento del orden público. Asimismo, participará con voz y voto un representante de la asociación de Entidades Locales de mayor implantación a nivel nacional en las reuniones.

Por decisión de su presidente, podrán asistir aquellas otras Administraciones Públicas, organismos o expertos cuyo asesoramiento técnico se estime preciso en razón de los temas a tratar.

4. El Grupo de Trabajo se reunirá al menos dos veces al año, con carácter ordinario, y de forma extraordinaria cuando así se considere oportuno a convocatoria de su Presidente, quien determinará el orden del día de la reunión. La secretaría radicará en uno de los funcionarios que prestan servicios en el CNPIC, por decisión de su Director.

5. Para el ejercicio de las competencias que este reglamento atribuye al Grupo de Trabajo, podrán constituirse otros grupos de trabajo sectoriales para los sectores o subsectores incluidos en el anexo de la Ley 8/2011, de 28 de abril, en los que podrán participar, además del CNPIC y el correspondiente ministerio u organismo del Sistema, los operadores críticos y otros agentes del Sistema.

Artículo 13. *Operadores Críticos.*

1. Los operadores críticos serán los agentes integrantes del Sistema, que, procedentes tanto del sector público como del sector privado, reúnan las condiciones establecidas en el artículo 13 de la Ley 8/2011, de 28 de abril.

2. En aplicación de lo previsto en la citada Ley, corresponde a los operadores críticos:

a) Prestar su colaboración técnica a la Secretaría de Estado de Seguridad, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo. Por ello, deberán actualizar los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento o previa validación del CNPIC.

b) Colaborar, en su caso, con el Grupo de Trabajo, en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador y proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo que establece el Capítulo III, Título III del presente reglamento.

d) Elaborar un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo así como proceder a su actualización periódicamente o cuando las circunstancias así lo exijan, conforme a lo establecido en el Capítulo IV, Título III del presente reglamento.

e) Designar a un Responsable de Seguridad y Enlace, en virtud de lo dispuesto en el artículo 34 del presente reglamento.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por la Secretaría de Estado de Seguridad, comunicando su designación a los órganos correspondientes en virtud de lo dispuesto en el artículo 35 del presente reglamento.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial, en el marco de lo establecido en el Título III de este reglamento.

Artículo 14. *Designación de los operadores críticos.*

1. Para la designación de una empresa u organismo como operador crítico, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica, en aplicación de los criterios previstos en el artículo 2, apartado h), de la Ley 8/2011, de 28 de abril. En tal caso, el CNPIC, elaborará una propuesta de resolución y la notificará al titular o administrador de aquéllas.

2. La citada propuesta contendrá la intención de designar al titular o administrador de la instalación o instalaciones como operador crítico.

3. El interesado dispondrá de un plazo de quince días a contar desde el día siguiente a la recepción de la notificación para remitir al CNPIC las alegaciones que considere procedentes, transcurrido el cual la Comisión, a propuesta del Grupo de Trabajo, dictará la resolución en la que se designará, en su caso, a dicho operador, como crítico. Esta resolución podrá ser recurrida en alzada ante el Secretario de Estado de Seguridad, y, eventualmente, con posterioridad, ante la jurisdicción contencioso-administrativa, en los términos generales previstos en la legislación vigente en materia de procedimiento administrativo y del orden jurisdiccional contencioso-administrativo.

4. Las comunicaciones con el interesado tendrán en cuenta, en todo caso, la clasificación de seguridad que corresponda según la normativa vigente.

Artículo 15. *Interlocución con los operadores críticos.*

1. Los operadores críticos del Sector Privado tendrán en el CNPIC el punto directo de interlocución con la Secretaría de Estado de Seguridad en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto este reglamento.

2. En aquellos casos en que los operadores críticos del Sector Público estén vinculados o dependan de una Administración pública, el órgano de dicha Administración que ostente competencias por razón de la materia podrá constituirse en el interlocutor con el Ministerio del Interior a través del CNPIC en lo relativo a las responsabilidades, funciones y obligaciones recogidas en la Ley 8/2011, de 28 de abril, y en lo previsto en este reglamento, debiendo comunicar dicha decisión al CNPIC.

TÍTULO III

Instrumentos de planificación

CAPÍTULO I

El Plan Nacional de Protección de las Infraestructuras Críticas

Artículo 16. *Finalidad, elaboración y contenido.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas es el instrumento de programación del Estado elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

2. El Plan Nacional de Protección de las Infraestructuras Críticas establecerá los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para asegurar la protección permanente, actualizada y homogénea de nuestro sistema de infraestructuras estratégicas frente a las amenazas provenientes de ataques deliberados contra ellas.

3. Asimismo, el Plan preverá distintos niveles de seguridad e intervención policial, que se activarán, en cada caso, en función de los resultados de la evaluación de la amenaza y coordinadamente con el Plan de Prevención y Protección Antiterrorista en vigor, al cual deberá adaptarse.

Los distintos niveles de seguridad contendrán la adopción graduada de dispositivos y medidas de protección ante situaciones de incremento de la amenaza contra las infraestructuras estratégicas nacionales y requerirán el concurso de las Fuerzas y Cuerpos de Seguridad, las Fuerzas Armadas, en su caso, y los responsables de los organismos o titulares o gestores de las infraestructuras a proteger.

Artículo 17. *Aprobación, registro y clasificación.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será aprobado por resolución del titular de la Secretaría de Estado de Seguridad y quedará registrado en el CNPIC, sin perjuicio de que aquellos otros organismos que necesiten conocer del mismo sean autorizados para acceder a él por el Secretario de Estado de Seguridad.

2. El Plan estará clasificado conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente tal clasificación en el instrumento de su aprobación.

Artículo 18. *Revisión y actualización.*

1. El Plan Nacional de Protección de las Infraestructuras Críticas será revisado cada cinco años por la Secretaría de Estado de Seguridad.
2. La modificación de alguno de los datos o instrucciones incluidos en el Plan Nacional de Protección de las Infraestructuras Críticas obligará a la automática actualización del mismo, que se llevará a cabo por el CNPIC y requerirá la aprobación expresa del Secretario de Estado de Seguridad.

CAPÍTULO II

Los Planes Estratégicos Sectoriales

Artículo 19. *Finalidad, elaboración y contenido.*

1. Los Planes Estratégicos Sectoriales son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los sectores contemplados en el anexo de la Ley 8/2011, de 28 de abril, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.

2. El Grupo de Trabajo, coordinado por el CNPIC, elaborará con la participación y asesoramiento técnico de los operadores afectados, en su caso, un Plan Estratégico por cada uno de los sectores o subsectores de actividad que se determinen.

3. Los Planes Estratégicos Sectoriales estarán basados en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.

4. Cada Plan Estratégico Sectorial contendrá, como mínimo, los siguientes extremos:

- a) Análisis de riesgos, vulnerabilidades y consecuencias a nivel global.
- b) Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.
- c) Propuestas de implantación de otras medidas preventivas y de mantenimiento (por ejemplo, ejercicios y simulacros, preparación e instrucción del personal, articulación de los canales de comunicación precisos, planes de evacuación o planes operativos para abordar posibles escenarios adversos).
- d) Medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

5. Los Planes Estratégicos Sectoriales podrán constituirse teniendo en cuenta otros planes o programas ya existentes, creados sobre la base de su propia legislación específica sectorial. Cuando los referidos planes o programas sectoriales reúnan los extremos a los que se refiere el apartado cuarto, podrán adoptarse los mismos como Plan Estratégico Sectorial del sector o subsector correspondiente.

Artículo 20. *Aprobación, registro y clasificación.*

1. Los Planes Estratégicos Sectoriales deberán ser aprobados por la Comisión en el plazo máximo de doce meses a partir de la entrada en vigor del presente real decreto.

2. El CNPIC gestionará y custodiará un registro central de todos los Planes Estratégicos Sectoriales existentes, una vez éstos sean aprobados por la Comisión. Los ministerios y organismos del Sistema tendrán acceso a los Planes de aquellos sectores para los que sean competentes.

3. Los Planes Estratégicos Sectoriales estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes.

Artículo 21. *Revisión y actualización.*

1. Los Planes Estratégicos Sectoriales deberán ser revisados cada dos años por los ministerios y organismos del Sistema.
2. La modificación de alguno de los datos incluidos en los Planes Estratégicos Sectoriales obligará a la automática actualización de éstos, que se llevará a cabo por los ministerios y organismos del Sistema que sean competentes en el sector afectado y será posteriormente aprobada por la Comisión.

CAPÍTULO III

Los Planes de Seguridad del Operador

Artículo 22. *Finalidad, elaboración y contenido.*

1. Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.
2. En el plazo de seis meses a partir de la notificación de la resolución de su designación, cada operador crítico deberá haber elaborado un Plan de Seguridad del Operador y presentarlo al CNPIC, que lo evaluará y lo informará para su aprobación, si procede, por el Secretario de Estado de Seguridad u órgano en el que éste delegue.
3. Los Planes de Seguridad del Operador deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos.
4. La Secretaría de Estado de Seguridad del Ministerio del Interior, a través del CNPIC, establecerá, con la colaboración de los Ministerios del Sistema y organismos dependientes, los contenidos mínimos de los Planes de Seguridad del Operador, así como el modelo en el que basar la elaboración de éstos.

Artículo 23. *Aprobación, registro y clasificación.*

1. El Secretario de Estado de Seguridad, u órgano en el que éste delegue, previo informe del CNPIC, aprobará el Plan de Seguridad del Operador o las propuestas de mejora del mismo, notificando la resolución al interesado en el plazo máximo de dos meses.
2. Junto a la resolución de aprobación o modificación, el CNPIC, tomando en su caso como referencia las actuaciones del organismo regulador competente en virtud de la normativa sectorial aplicable, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar.
3. El CNPIC gestionará y custodiará un registro central de todos los Planes de Seguridad del Operador existentes, una vez éstos sean aprobados por el Secretario de Estado de Seguridad. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.
4. Los Planes de Seguridad del Operador estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los operadores críticos responsables de la elaboración de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 24. *Revisión y actualización.*

1. Los Planes de Seguridad del Operador deberán ser revisados cada dos años por los operadores críticos y aprobados por el CNPIC. Éste podrá requerir en cualquier momento información concreta sobre el estado de implantación del Plan de Seguridad del Operador.

2. La modificación de alguno de los datos incluidos en los Planes de Seguridad del Operador obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

CAPÍTULO IV

Los Planes de Protección Específicos

Artículo 25. *Finalidad, elaboración y contenido.*

1. Los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

2. En el plazo de cuatro meses a partir de la aprobación del Plan de Seguridad del Operador, cada operador crítico deberá haber elaborado un Plan de Protección Específico por cada una de sus infraestructuras críticas así consideradas por la Secretaría de Estado de Seguridad y presentarlo al CNPIC. Igual procedimiento y plazos se establecerán cuando se identifique una nueva infraestructura crítica.

3. Los Planes de Protección Específicos de las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información.

4. Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas.

5. La Secretaría de Estado de Seguridad, a través del CNPIC, establecerá los contenidos mínimos de los Planes de Protección Específicos, así como el modelo en el que fundamentar la estructura y la compleción de éstos que, en todo caso, cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador.

Artículo 26. *Aprobación, registro y clasificación.*

1. La Secretaría de Estado de Seguridad notificará al interesado, en el plazo máximo de dos meses contados a partir de la recepción, su resolución con la aprobación de los diferentes Planes de Protección Específicos o de las eventuales propuestas de mejora de éstos. Previamente, a través del CNPIC, se recabará informe preceptivo de las Delegaciones del Gobierno en las respectivas Comunidades Autónomas o en las Ciudades con Estatuto de Autonomía en el que se considerará, en su caso, el criterio de los órganos competentes de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, así como del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. Junto a la resolución de aprobación o modificación, el CNPIC, basándose en los informes mencionados en el punto anterior, efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de preferencia de las medidas y los procedimientos a adoptar sobre las infraestructuras afectadas.

3. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean aprobados por el Secretario de Estado de Seguridad, todos los Planes de Protección Específicos de las infraestructuras críticas o infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro

central de todos los Planes de Protección Específicos existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

4. Los Planes de Protección Específicos estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración de los respectivos planes y aquellos encargados de su registro deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 27. *Revisión y actualización.*

1. Los Planes de Protección Específicos deberán ser revisados cada dos años por los operadores críticos, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, y por el CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Protección Específicos obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.

Artículo 28. *Aplicación y seguimiento.*

1. Los Delegados del Gobierno en las Comunidades Autónomas velarán por la correcta ejecución de los diferentes Planes de Protección Específicos y tendrán facultades de inspección en el ámbito de la protección de infraestructuras críticas. Dichas facultades deberán desarrollarse, en su caso, de forma coordinada con las facultades inspectoras del órgano u organismo competente para otorgar a los operadores críticos las autorizaciones correspondientes según la legislación sectorial vigente.

2. En aquellas Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, las facultades de inspección serán ejercidas por sus órganos competentes, sin perjuicio de lo dispuesto en la legislación sectorial aplicable y de la necesaria coordinación con las Delegaciones del Gobierno en dichas Comunidades y los otros organismos reguladores competentes en virtud de su normativa sectorial.

3. En ejercicio de ese seguimiento, los organismos competentes podrán en todo momento requerir del responsable de las infraestructuras críticas o infraestructuras críticas europeas la situación actualizada de la implantación de las medidas propuestas en las resoluciones de aprobación o modificación de los Planes de Protección Específicos elaborados en caso de variación de las circunstancias que determinaron su adopción, o bien para adecuarlos a la normativa vigente que les afecte, dando cuenta del resultado de ello a la Secretaría de Estado de Seguridad, a través del CNPIC.

4. Las facultades de inspección en las instalaciones portuarias, así como en aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, serán establecidas de acuerdo con lo previsto en el Real Decreto 1617/2007, de 7 de diciembre.

Artículo 29. *Compatibilidad con otros planes existentes.*

1. La elaboración de los Planes de Protección Específicos para cada una de las infraestructuras críticas se efectuará sin perjuicio del obligado cumplimiento de lo exigido por el Código Técnico de la Edificación, aprobado por el Real Decreto 314/2006, de 17 de marzo, el Real Decreto 393/2007, de 23 de marzo, por el que se aprueba la Norma Básica de Autoprotección de los centros, establecimientos y dependencias dedicados a actividades que puedan dar origen a situaciones de emergencia, la normativa de Seguridad Privada o cualquier otra reglamentación sectorial específica que le sea de aplicación.

2. Las instalaciones Nucleares e Instalaciones Radiactivas que se consideren críticas reguladas en el Reglamento sobre instalaciones nucleares y radiactivas, aprobado por el Real Decreto 1836/1999 de 3 de diciembre, modificado por el Real Decreto 35/2008 de 18 de enero, integrarán sus Planes de Protección Específicos en los respectivos Planes de Protección Física rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en su normativa sectorial específica, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

3. Las instalaciones portuarias, así como aquellos otros puntos o establecimientos considerados críticos que se encuentren integrados en un puerto, conforme a lo dispuesto en el Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y el transporte marítimo, integrarán sus Planes de Protección Específicos en los Planes de Protección de Puertos previstos en el citado Real Decreto rigiéndose, en lo relativo a su aprobación y evaluación, por lo establecido en esa norma, sin perjuicio de lo que le sea de aplicación según la Ley 8/2011, de 28 de abril.

4. En el caso de aeropuertos, aeródromos e instalaciones de navegación aérea se considerarán Planes de Protección Específicos los respectivos Programas de Seguridad de los aeropuertos aprobados conforme a lo dispuesto en la Ley 21/2003, de 7 de julio, de Seguridad Aérea modificada por la Ley 1/2011, de 4 de marzo por la que se establece el Programa Estatal de Seguridad Operacional para la Aviación Civil y se modifica la Ley 21/2003, de 7 de julio de Seguridad Aérea y en el Real Decreto 550/2006, de 5 de mayo, por el que se designa la autoridad competente responsable de la coordinación y seguimiento del Programa Nacional de Seguridad para la Aviación Civil y se determina la organización y funciones del Comité Nacional de Seguridad de la Aviación Civil. No obstante, el Ministerio del Interior, a través de su representante en el Comité Nacional de Seguridad de la Aviación Civil podrá proponer contenidos adicionales, de conformidad con lo establecido en el artículo 25, apartado quinto de este real decreto.

CAPÍTULO V

Los Planes de Apoyo Operativo

Artículo 30. *Finalidad, elaboración y contenido.*

1. Los Planes de Apoyo Operativo son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

2. Por cada una de las infraestructuras críticas e infraestructuras críticas europeas dotadas de un Plan de Protección Específico y sobre la base a los datos contenidos en éste, la Delegación del Gobierno en la Comunidad Autónoma o, en su caso, el órgano competente de la Comunidad Autónoma, supervisará la realización de un Plan de Apoyo Operativo por parte del Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate. Para su elaboración, que deberá realizarse en un plazo de cuatro meses a partir de la aprobación del respectivo Plan de Protección Específico, se contará con la colaboración del responsable de seguridad de la infraestructura.

3. Sobre la base de sus correspondientes Planes de Protección Específicos, los Planes de Apoyo Operativo deberán contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos.

4. El CNPIC establecerá los contenidos mínimos de los Planes de Apoyo Operativo, así como el modelo en el que fundamentar la estructura y desarrollo de éstos, que se basarán en la parte que les corresponda en la información contenida en los respectivos Planes de Protección Específicos.

5. El Ministerio de Defensa podrá acceder a los Planes de Apoyo Operativo de aquellas infraestructuras críticas o infraestructuras críticas europeas que, en caso de activarse el Plan Nacional de Protección de las Infraestructuras Críticas y a los efectos de coordinar los correspondientes apoyos de las Fuerzas Armadas, se considere oportuno, previo estudio conjunto de los mencionados apoyos.

Artículo 31. *Aprobación, registro y clasificación.*

1. Los Planes de Apoyo Operativo serán validados y aprobados por la Secretaría de Estado de Seguridad, a través del CNPIC.

2. Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, el órgano competente de cada Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, mantendrán un registro donde obren, una vez sean validados, todos los Planes de Apoyo Operativo de las infraestructuras críticas e infraestructuras críticas europeas localizadas en su demarcación, y que deberán mantener permanentemente actualizado. En cualquier caso y sobre la base de lo anterior, el CNPIC gestionará y custodiará un registro central de todos los Planes de Apoyo Operativo existentes. Los agentes del Sistema podrán tener acceso a los planes, previa comprobación por el CNPIC de su necesidad de conocer y con la autorización correspondiente.

3. Los Planes de Apoyo Operativo estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o a parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los agentes del Sistema responsables de la elaboración y registro de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.

Artículo 32. *Revisión y actualización.*

1. Los Planes de Apoyo Operativo deberán ser revisados cada dos años por el Cuerpo Policial estatal, o en su caso autonómico, con competencia en la demarcación territorial de que se trate, revisión que deberá ser aprobada por las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, por el órgano competente de las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público, requiriendo la aprobación expresa del CNPIC.

2. La modificación de alguno de los datos incluidos en los Planes de Apoyo Operativo obligará a la automática actualización de éstos, que se llevará a cabo mediante el procedimiento previsto en el apartado primero.

TÍTULO IV

Comunicaciones entre los operadores críticos y las Administraciones públicas

Artículo 33. *Seguridad de las comunicaciones.*

1. El CNPIC será el responsable de administrar los sistemas de gestión de la información y comunicaciones que se diseñen en el ámbito de la protección de las infraestructuras críticas, que deberá contar para ello con el apoyo y colaboración de los agentes del Sistema y de todos aquellos otros organismos o entidades afectados.

2. La seguridad de los sistemas de información y comunicaciones previstos en este real decreto será acreditada y, en su caso, certificada por el Centro Criptológico Nacional del Centro Nacional de Inteligencia, de acuerdo con las competencias establecidas en su normativa específica.

3. La Presidencia del Gobierno facilitará el uso de la Malla B, sistema soporte de comunicaciones estratégicas seguras del Sistema Nacional de Gestión de Crisis y de la Presidencia del Gobierno, a través del cual los agentes del Sistema autorizados podrán

acceder a la información disponible en el Catálogo, con los niveles de acceso que se determinen.

Artículo 34. *El Responsable de Seguridad y Enlace.*

1. En el plazo de tres meses desde su designación como operadores críticos, los mismos nombrarán y comunicarán a la Secretaría de Estado de Seguridad, a través del CNPIC, el nombre del Responsable de seguridad y enlace en los términos y con los requisitos previstos por el artículo 16 de la Ley 8/2011, de 28 de abril.

2. El Responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto.

Artículo 35. *El Delegado de Seguridad de la infraestructura crítica.*

1. En el plazo de tres meses desde la identificación como crítica o crítica europea, de una de sus infraestructuras, los operadores críticos comunicarán a las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia e identidad de un Delegado de Seguridad para dicha infraestructura.

2. El Delegado de Seguridad constituirá el enlace operativo y el canal de información con las autoridades competentes en todo lo referente a la seguridad concreta de la infraestructura crítica o infraestructura crítica europea de que se trate, encauzando las necesidades operativas e informativas que se refieran a aquélla.

Artículo 36. *Seguridad de los datos clasificados.*

Los datos clasificados relativos a las infraestructuras de los operadores críticos cumplirán, en todo caso, con los requerimientos de seguridad establecidos por el Secretario de Estado Director del Centro Nacional de Inteligencia, de acuerdo con la normativa específica aplicable.

§ 18

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems*)», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

- a) Seguridad como proceso integral.
- b) Gestión de la seguridad basada en los riesgos.
- c) Prevención, detección, respuesta y conservación.
- d) Existencia de líneas de defensa.
- e) Vigilancia continua.
- f) Reevaluación periódica.
- g) Diferenciación de responsabilidades.

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 9. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

- a) Los objetivos o misión de la organización.
- b) El marco regulatorio en el que se desarrollarán las actividades.
- c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
- d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.
- e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

- a) El responsable de la información determinará los requisitos de la información tratada
- b) El responsable del servicio determinará los requisitos de los servicios prestados.
- c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.

5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
- c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 27. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

- a) Los activos que constituyen los sistemas de información concernidos.
- b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
- c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurren impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team*), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team*, en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoría de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Disposición adicional primera. *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de dicha Secretaría de Estado.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

Disposición transitoria única. *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

- a) Confidencialidad [C].
- b) Integridad [I].
- c) Trazabilidad [T].
- d) Autenticidad [A].
- e) Disponibilidad [D].

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

- 1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño menor en los activos de la organización.
- 3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
- 4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
- 5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

- 1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño significativo en los activos de la organización.
- 3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
- 4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
- 5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

- 1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
- 2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
- 3.º El incumplimiento grave de alguna ley o regulación.
- 4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
- 5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.

c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

ANEXO II

Medidas de Seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

- a) Las dimensiones de seguridad relevantes en el sistema a proteger.
- b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

- a) Identificación de los tipos de activos presentes.
- b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
- c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
- d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
- e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
		BAJO	MEDIO	ALTO
		Categoría de seguridad del sistema		
		BÁSICA	MEDIA	ALTA
org Marco organizativo				
org.1 Política de seguridad	Categoría	aplica	aplica	aplica
org.2 Normativa de seguridad	Categoría	aplica	aplica	aplica

ÁMBITOS DE LA SEGURIDAD NACIONAL: CIBERSEGURIDAD

§ 18 Esquema Nacional de Seguridad

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
		BAJO	MEDIO	ALTO	
		Categoría de seguridad del sistema			
		BÁSICA	MEDIA	ALTA	
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	Marco operacional				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

Medidas de Seguridad	Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
		BAJO	MEDIO	ALTO	
		Categoría de seguridad del sistema			
		BÁSICA	MEDIA	ALTA	
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

- [org.1.1] Los objetivos o misión de la organización.
- [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
- [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
- [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

- Categoría BÁSICA: org.1.
- Categoría MEDIA: org.1.
- Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

- [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: org.2.
- Categoría MEDIA: org.2.
- Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- [org.3.1] Cómo llevar a cabo las tareas habituales.
- [org.3.2] Quién debe hacer cada tarea.
- [org.3.3] Cómo identificar y reportar comportamientos anómalos.
- [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

- a) Su control de acceso.
- b) Su almacenamiento.
- c) La realización de copias.
- d) El etiquetado de soportes.
- e) Su transmisión telemática.
- f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

- Categoría BÁSICA: org.3.
- Categoría MEDIA: org.3.
- Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

- [org.4.1] Utilización de instalaciones, habituales y alternativas.
- [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- [org.4.3] Entrada de aplicaciones en producción.
- [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
- [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
- [org.4.6] Utilización de soportes de información.
- [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
- [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

- Categoría BÁSICA: org.4.
- Categoría MEDIA: org.4.
- Categoría ALTA: org.4.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

- [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
- [op.pl.1.2] Identifique las amenazas más probables.
- [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

- [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r1.2] Cuantifique las amenazas más probables.
- [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

- [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r2.2] Cuantifique las amenazas posibles.
- [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
- [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.1.
- Categoría MEDIA: op.pl.1 + R1.
- Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

- [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
- [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
- [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.2.
- Categoría MEDIA: op.pl.2 + R1.
- Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

- [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
- [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
- [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.3.
- Categoría MEDIA: op.pl.3.
- Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

- [op.pl.4.1] Necesidades de procesamiento.
- [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- [op.pl.4.3] Necesidades de comunicación.
- [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
- [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

- [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
- [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

- Nivel BAJO: op.pl.4.
- Nivel MEDIO: op.pl.4 + R1.
- Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

- [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.pl.5.
- Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.

– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

- Nivel BAJO: op.acc.1.
- Nivel MEDIO: op.acc.1 +R1.
- Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.

– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.2.
- Nivel MEDIO: op.acc.2.
- Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.

– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

- [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunar funciones de configuración y mantenimiento del sistema.
- [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

- [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

- [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.acc.3.
- Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
- [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
- [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.4.
- Nivel MEDIO: op.acc.4.
- Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A
-------------	---------

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

– [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.

– [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

– [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

– [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

- [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
- [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
- Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
- Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.

– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.

– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).

– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.

– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.

– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.

b) El tráfico deberá ser cifrado.

§ 18 Esquema Nacional de Seguridad

- c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.
- d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
- Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
- Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

- [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

- [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

- [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

- [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: op.exp.1.
- Categoría MEDIA: op.exp.1.
- Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

- [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
- [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.

b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.

c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.

– Categoría MEDIA: op.exp.2.

– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).

– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).

– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).

– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).

– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).

– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.

– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.

– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.

– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.3.
- Categoría MEDIA: op.exp.3 + R1.
- Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.

– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.

– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).

3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.4.
- Categoría MEDIA: op.exp.4 + R1.
- Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

- [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.

- [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.

- [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.

- [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.

- [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

- [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.

- [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.

- [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.exp.5.
- Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.

- [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
- [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
- [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
- [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
- [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

- [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

- [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

- [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

- [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

- [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
- [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.6.
- Categoría MEDIA: op.exp.6+ R1 + R2.
- Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

- [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
- [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.

– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.

b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.

– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.

– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.

– Categoría MEDIA: op.exp.7+ R1 + R2.

– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.

– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.

– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.

– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.

– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.9.
- Categoría MEDIA: op.exp.9.
- Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

- [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
- [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
- [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

- [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

- [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.10.
- Categoría MEDIA: op.exp.10 + R1.
- Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.1.
- Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

- [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
- [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.2.
- Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

- [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
- [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
- [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

- [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
- [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

- [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

- [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: no aplica.
- Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.ext.4.
- Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.

– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

- a) Auditoría de pruebas de penetración (*pentesting*).
- b) Transparencia.
- c) Cifrado y gestión de claves.
- d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

- Categoría BÁSICA: op.nub.1.
- Categoría MEDIA: op.nub.1 + R1.
- Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.cont.1.
- Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

- [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
- [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
- [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

- [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

- a) Servicios contratados a terceros.
- b) Instalaciones alternativas.
- c) Personal alternativo.
- d) Equipamiento informático alternativo.
- e) Medios de comunicación alternativos.

- [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.

- [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

- [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoria	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

- [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

- [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

- [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

- [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.1.
- Categoría MEDIA: op.mon.1 + R1.
- Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoria	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

- [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

- [op.mon.2.r1.1] Se recopilarán los datos precisos que permitan evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

- [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

- Categoría BÁSICA: op.mon.2.
- Categoría MEDIA: op.mon.2 + R1+ R2.
- Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoria	BÁSICA	MEDIA	ALTA

aplica + R1+R2 + R1+R2+R3+R4+R5+R6

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.

– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.

– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.

– [op.mon.3.r6.2] Análisis de vulnerabilidades.

– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.

– Categoría MEDIA: op.mon.3 + R1 + R2.

– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
- [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.1.
- Categoría MEDIA: mp.if.1.
- Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.2.
- Categoría MEDIA: mp.if.2.
- Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

- [mp.if.3.1] Las condiciones de temperatura y humedad.
- [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
- [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

- Categoría BÁSICA: mp.if.3.
- Categoría MEDIA: mp.if.3.
- Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.4.
- Nivel MEDIO: mp.if.4 + R1.
- Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: mp.if.5.
- Nivel MEDIO: mp.if.5.
- Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.if.6.
- Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

§ 18 Esquema Nacional de Seguridad

- Categoría BÁSICA: mp.if.7.
- Categoría MEDIA: mp.if.7.
- Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.

– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.per.1.
- Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

- [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
- [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
- [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
- [mp.per.2.4] En caso de personal contratado a través de un tercero:
 - [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
 - [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

- [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.2.
- Categoría MEDIA: mp.per.2 + R1.
- Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

- [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.3.
- Categoría MEDIA: mp.per.3.
- Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

- Configuración de sistemas.
- Detección y reacción ante incidentes.
- Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.per.4.
- Categoría MEDIA: mp.per.4.
- Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.1.
- Categoría MEDIA: mp.eq.1 + R1.
- Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.eq.2.
- Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

- [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
- [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

- Categoría BÁSICA: mp.eq.3.
- Categoría MEDIA: mp.eq.3.
- Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

- a) Dispositivos multifunción: impresoras, escáneres, etc.
- b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
- c) Dispositivos internet de las cosas, en inglés *Internet of Things (IoT)*.
- d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device (BYOD)*.
- e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.eq.4.
- Nivel MEDIO: mp.eq.4 + R1.
- Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
- [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

- Categoría BÁSICA: mp.com.1.
- Categoría MEDIA: mp.com.1.
- Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

- [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

- [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

- [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

- [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

- [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

- [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.com.2.

- Nivel MEDIO: mp.com.2 + R1.
- Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).

– [mp.com.3.2] Se prevendrán ataques garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

- a) La alteración de la información en tránsito.
- b) La inyección de información espuria.
- c) El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.com.3.
- Nivel MEDIO: mp.com.3 + R1 + R2.
- Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+ [R1oR2oR3]	+ [R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

- [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
- [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

- [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
- [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

- Usuarios.
- Servicios.
- Administración.

Refuerzo R2-Segmentación lógica avanzada.

- [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

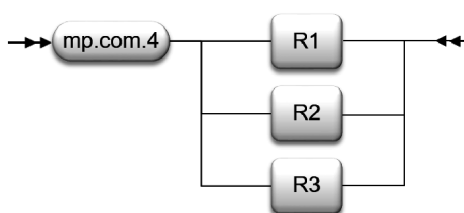
- [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

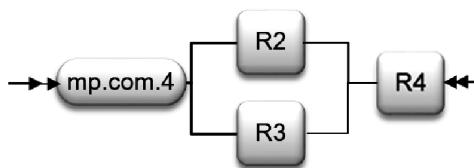
- [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
- [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



- Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

§ 18 Esquema Nacional de Seguridad

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.

– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.

– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.si.1.
- Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias de seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.si.2.
- Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

- [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
- [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

- Categoría BÁSICA: mp.si.3.
- Categoría MEDIA: mp.si.3.
- Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

- [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
- [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
- [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
- [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

- Categoría BÁSICA: mp.si.4.
- Categoría MEDIA: mp.si.4.
- Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

- [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

- [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

- [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.si.5.
- Nivel MEDIO: mp.si.5 + R1.
- Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

- [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

- [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

- [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:
 - Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
 - Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
 - Tratará específicamente los datos usados en pruebas.
 - Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

- [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:
 - Los mecanismos de identificación y autenticación.
 - Los mecanismos de protección de la información tratada.
 - La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

- [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

- [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
- Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

- [mp.sw.2.1] Se comprobará que:
 - a) Se cumplen los criterios de aceptación en materia de seguridad.
 - b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

- [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

- [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

- Categoría BÁSICA: mp.sw.2.
- Categoría MEDIA: mp.sw.2 + R1.
- Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.info.1.
- Categoría MEDIA: mp.info.1.
- Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

- [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
- [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.info.2.
- Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

- [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

- [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

- [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

- [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

- Nivel BAJO: mp.info.3.
- Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
- Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

- [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
- [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
- [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
- [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

- [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
- [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: no aplica.
- Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

- Nivel BAJO: mp.info.5.
- Nivel MEDIO: mp.info.5.
- Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

- [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.

- [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

- a) Frecuencia de las copias.
- b) Requisitos de almacenamiento en el propio lugar.
- c) Requisitos de almacenamiento en otros lugares.
- d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

- [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

- [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

- Nivel BAJO: mp.info.6.
- Nivel MEDIO: mp.info.6+ R1.
- Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
- [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

- [mp.s.1.3] Correo no solicitado, en su expresión inglesa «spam».
- [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
- [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «applet».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

- [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
- [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.1.
- Categoría MEDIA: mp.s.1.
- Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+[R1oR2]	+[R1oR2]	+R2+R3

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

- [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).

c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.

d) Se prevendrán ataques de inyección de código.

- [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.

- [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.

– [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.

– [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.

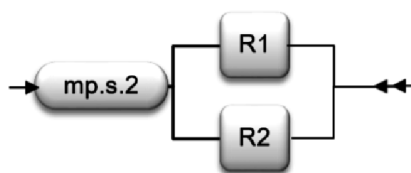
– [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

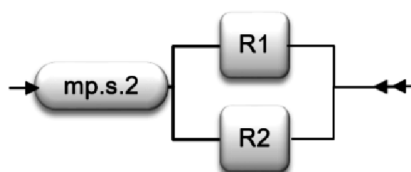
– [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

- Categoría BÁSICA: mp.s.2 + [R1 o R2].



- Categoría MEDIA: mp.s.2 + [R1 o R2].



- Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
- [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
- [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
- [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
- [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
- [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
- [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

- [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
- [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

- [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

- Categoría BÁSICA: mp.s.3.
- Categoría MEDIA: mp.s.3.
- Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS* y *Distributed Denial of Service, DDoS*). Para ello:

- [mp.s.4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
- [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

- [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
- [mp.s.4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

- [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: mp.s.4.
- Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM*) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, éstas se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.

b) Que existen procedimientos para resolución de conflictos entre dichos responsables.

c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».

d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.

e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.

f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

a) Documentación de los procedimientos.

b) Registro de incidentes.

c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.

El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.

b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

- Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.
- Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.
- Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.
- Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.
- Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.
- Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.
- Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.
- Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.
- Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.
- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Dispositivo de autenticación (*token*): autenticador físico.
- Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.
- Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.
- Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:
 - a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
 - b) Servidor central (host), frontal Unix y equipos administrativos.
 - c) Seguridad física, seguridad lógica.
- Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

- Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.
- Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.
- Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
- Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.
- Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.
- Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.
- Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.
- Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.
- Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.
- Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.
- Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.
- PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.
- Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.
- Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
- Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.
- Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

– Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.

– Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.

– Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.

– Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.

– Sistema de información: cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

– TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

– USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

– Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.