III. OTRAS DISPOSICIONES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

8109 *Orden ETD/305/2023, de 16 de marzo, por la que se aprueba la política de seguridad de la información del Ministerio de Asuntos Económicos y Transformación Digital.*

El marco de la relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos, se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Por otra parte, el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de dicha norma, estando constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada. Esta disposición ha sido desarrollada a través del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El Real Decreto 311/2022, de 3 de mayo, tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. Su artículo 12.3 exige que, en la Administración General del Estado, cada ministerio cuente con su política de seguridad, que aprobará la persona titular del Departamento. Dicha política se establecerá con base en los principios básicos recogidos en el capítulo II del real decreto (seguridad como proceso integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua; reevaluación periódica; diferenciación de responsabilidades). Por su parte, su artículo 13 exige que la política de seguridad identifique unos claros responsables de velar por su cumplimiento.

En este marco normativo, la presente orden tiene por objeto la aprobación de la Política de Seguridad de la Información del Ministerio de Asuntos Económicos y Transformación Digital. Para su elaboración se han tenido en cuenta, además de la normativa ya citada, las recomendaciones y guías del Centro Criptológico Nacional (guías STIC-800 relacionadas con el Esquema Nacional de Seguridad).

Desde el punto de vista del contenido ha de destacarse, en primer lugar, el artículo 5 que recoge los principios de la seguridad de la información, tanto los básicos, los cuales habrán de tenerse en cuenta en cualquier actividad relacionada con el uso de los activos de la información, como los particulares, que garantizan el cumplimiento de los primeros. En segundo lugar, ha de mencionarse la creación, en el artículo 7, del Comité de Dirección de Seguridad de la Información, órgano adscrito a la Subsecretaría del Departamento y que tiene entre sus funciones aprobar las propuestas de modificación y actualización permanente que se hagan sobre la Política de Seguridad de la Información. Dicho órgano colegiado será asistido por el grupo de trabajo que se define en el artículo 8. Por otra parte, en los artículos 9 al 13 se definen todos roles y responsabilidades de cada uno de los participantes los procesos de definición, ejecución, y evaluación de las medidas de seguridad que se deben implantar en los órganos y organismos que formen parte del ámbito de aplicación de la Política de Seguridad de la Información. La gestión de los riesgos es la herramienta fundamental para garantizar la seguridad de la información en cualquier organización, y en este sentido el artículo 15 define el proceso de gestión de riesgos como una metodología general, así como las actividades y responsabilidades a la hora de ejecutar los diferentes análisis de riesgos.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

Además, el artículo 16 define los tres niveles normativos que se utilizarán para articular la Política de Seguridad de la Información, de forma que se pueda disponer de un corpus normativo común para todos los órganos y organismos que formen parte del ámbito de la Política de Seguridad de la Información.

Dentro de los principios particulares ha de resaltarse el de la protección de los datos de carácter personal, que además tiene una regulación específica en el artículo 17, lo que permitirá garantizar de forma consistente en la presente norma, la seguridad de los tratamientos de datos personales en base al 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 o RGPD). En este sentido, la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reconoce al Esquema Nacional de Seguridad como un instrumento para la implementación de medidas que permitan garantizar la seguridad de los datos de carácter personal.

Por último, cabe reseñar la importancia de que el personal del Ministerio forme parte activa de ejecución de los mecanismos y buenas prácticas para garantizar la seguridad de la información en el ámbito corporativo. En particular, el artículo 19 reconoce la necesidad de que el personal cuente con la información y formación adecuadas, y conozca sus responsabilidades y deberes al respecto.

En la elaboración de la orden se han cumplido los principios de buena regulación recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, y en particular, los principios de necesidad y eficiencia, pues se trata del instrumento más adecuado para garantizar una política de seguridad en la utilización de medios electrónicos que permita una adecuada protección de la información dentro del Ministerio de Asuntos Económicos y Transformación Digital, evitando cargas administrativas innecesarias o accesorias. También se adecua al principio de proporcionalidad, pues no existe otra alternativa menos restrictiva de derechos o de obligaciones. En cuanto a los principios de seguridad jurídica y transparencia, se ha procurado la participación de las partes interesadas y la norma es coherente con el resto del ordenamiento jurídico.

Durante su tramitación se han recabado informes de la Comisión Ministerial de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, de la Agencia Española de Protección de Datos, y de la Secretaría General Técnica del Ministerio de Asuntos Económicos y Transformación Digital.

En su virtud, con la aprobación previa de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto.*

Constituye el objeto de esta orden la aprobación de la Política de Seguridad de la Información del Ministerio de Asuntos Económicos y Transformación Digital, en adelante PSI.

Artículo 2. *Ámbito de aplicación.*

1. El ámbito de aplicación inicial es el Ministerio de Asuntos Económicos y Transformación Digital. Sin embargo, se podrán adscribir a la presente PSI aquellos organismos públicos y entidades de derecho público vinculados o dependientes del Departamento, que no tengan establecida su propia PSI, y que así lo soliciten a la Subsecretaría de Asuntos Económicos y Transformación Digital.

2. Tal y como se dispone en el artículo 12.4 del Real Decreto 311/2022, de 3 de mayo, se excluye del ámbito de aplicación de la presente Orden a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, puesto que dicho órgano ya cuenta con su propia PSI.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

3. La PSI será de obligado cumplimiento para todo el personal que acceda, tanto a los sistemas de información, como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo. Lo dispuesto en esta norma también será de aplicación a los sistemas de información que traten información clasificada, pudiendo en este caso 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.

Artículo 3. *Misión del departamento.*

El Ministerio de Asuntos Económicos y Transformación Digital, de acuerdo con lo dispuesto en el artículo 1 del Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, es el departamento de la Administración General del Estado encargado de la propuesta, coordinación y ejecución de la política del Gobierno en materia económica, de apoyo a la empresa y de reformas para la mejora del crecimiento potencial y de la necesaria interlocución en estos asuntos con la Unión Europea y otros Organismos Económicos y Financieros Internacionales; así como de la política de telecomunicaciones y para la transformación digital, en particular impulsando la digitalización de las Administraciones Públicas. Igualmente le corresponde el establecimiento de las disposiciones y directrices necesarias para su funcionamiento, así como el resto de competencias y atribuciones que le confiere el ordenamiento jurídico.

Artículo 4. *Marco regulatorio.*

El marco normativo en que se desarrollan las actividades del Ministerio de Asuntos Económicos y Transformación Digital, en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

a) 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.
b) La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
c) La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
d) La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
e) 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.
f) El texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y su normativa de desarrollo.
g) El Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
h) El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que traspone la Directiva Europea NIS (Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016).
i) El 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.
j) El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

k) 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, de protección de datos de carácter personal.

l) El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

m) El Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

n) El Real Decreto 147/2021, de 9 de marzo, por el que se modifican el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

ñ) 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.

o) El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

p) La Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación centralizada.

q) La Orden ECC/523/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico del Ministerio de Economía y Competitividad.

r) La Orden ECC/131/2014, de 30 de enero, por la que se crean las sedes electrónicas del Ministerio de Economía y Competitividad.

s) La Orden ECE/91/2019, de 31 de enero, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Economía y Empresa y se regula su composición y funciones.

t) La 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.

u) La Orden PCM/466/2022, de 25 de mayo, por la que se publica el Acuerdo del Consejo de Ministros de 24 de mayo de 2022, por el que se aprueba el plan de medidas de ahorro y eficiencia energética de la Administración General del Estado y las entidades del sector público institucional estatal.

v) Aquellas normas aplicables a la administración electrónica y seguridad de la información que complementen, desarrollen o sustituyan a las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información del Ministerio.

Artículo 5. *Principios de la seguridad de la información.*

1. Principios básicos. Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Estos principios básicos, en su continuo fortalecimiento y revisión, se ajustarán en todo caso a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, así como a las guías CCN-STIC (publicaciones que el Centro Criptológico Nacional, tiene como cuerpo de guías de Seguridad de Tecnologías de la Información y de las Comunicaciones). Complementando lo dispuesto en el capítulo II del Real Decreto 311/2022, de 3 de mayo, se establecen los siguientes principios básicos:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad 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; y el responsable de la seguridad, que será distinto del responsable del sistema no debiendo existir dependencia jerárquica entre ambos, y que 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. En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamientos y, en su caso, al encargado de tratamiento, de acuerdo con las definiciones del artículo 4, apartados 7 y 8, del RGPD.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema de información, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de los Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Además, las medidas de seguridad deberán garantizar el cumplimiento de lo previsto en el artículo 32 del RGPD, por lo que el responsable del tratamiento de datos personales, y en su caso, de los encargados del tratamiento, podrán adoptar todas aquellas medidas adicionales con el fin de garantizar la seguridad de los datos personales, en virtud de lo dispuesto en el artículo 24 y 25 del RGPD, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y con dichas competencias entre sus funciones.

g) Seguridad desde el diseño y por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. Además, con el fin de garantizar la resiliencia y la protección de los datos personales, se deben tener en cuenta las medidas de seguridad por defecto en base a los artículos 24 y 25 del RGPD, así como las medidas de seguridad orientadas al riesgo según el artículo 32 del RGPD.

h) Vigilancia continua: de forma que la evaluación permanente del estado de la seguridad de los activos permita medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración. En cuanto la gestión de incidentes que afecten a datos personales, se tendrá en cuenta las obligaciones específicas de notificación, comunicación y documentación especificadas en los artículos 33 y 34 del RGPD.

2. Principios particulares y responsabilidades específicas. Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones del Departamento en dicha materia. Se establecen los siguientes principios particulares y responsabilidades específicas:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: Los activos de información del Departamento se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad. Para proteger las redes del Departamento, se analizará el tráfico cifrado de usuarios de forma automatizada. Se realizará la excepción en este análisis de las categorías de navegación relacionadas con datos sensibles especialmente protegidos de acuerdo con la normativa de protección de datos vigente, siempre que sea posible la discriminación.

f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

3. Sin perjuicio de lo establecido en los apartados 1 y 2, la presente PSI se establecerá en base a los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en el capítulo II y en el artículo 12.6 del Real Decreto 311/2022, de 3 de mayo.

4. Estos principios básicos, en su continuo fortalecimiento y revisión, se ajustarán en todo caso a las instrucciones técnicas de seguridad que publique la Secretaría de Estado de Digitalización de Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, así como a las guías CCN-STIC (publicaciones que el Centro Criptológico Nacional, tiene como cuerpo de guías de Seguridad de Tecnologías de la

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

Información y las Comunicaciones, tal y como se establece en la disposición adicional segunda del Real Decreto 311/2022, de 3 de mayo).

Artículo 6. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Asuntos Económicos y Transformación Digital está compuesta por los siguientes agentes:

a) El Comité de Dirección de Seguridad de la Información.
b) El Grupo de Trabajo Técnico de Seguridad de la Información.
c) Los Responsables de la Seguridad.
d) Los Responsables de la Información.
e) Los Responsables del Servicio.
f) Los Responsables del Sistema.
g) El Delegado de Protección de Datos.

Artículo 7. *Comité de Dirección de Seguridad de la Información.*

1. Se crea, adscrito a la Subsecretaría de Asuntos Económicos y Transformación Digital, el Comité de Dirección de Seguridad de la Información (en adelante, CDSI), como órgano colegiado de los previstos en el artículo 22.2 de la Ley 40/2015, de 1 de octubre, que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información.

2. El CDSI estará compuesto por los siguientes miembros:

a) Presidente/a: La persona titular de la Subsecretaría del Ministerio de Asuntos Económicos y Transformación Digital.

b) Vicepresidente/a: La persona titular de la Inspección de los Servicios del Ministerio de Asuntos Económicos y Transformación Digital.

c) Vocales:

i) Dos representantes por cada una de las Secretarías de Estado, designados por los titulares de dichos órganos superiores. Uno de los representantes propuesto por cada Secretaría de Estado deberá tener al menos rango de Subdirector/a General o equivalente.

ii) Además, se designarán hasta un máximo de tres Vocales de entre los organismos públicos adscritos al Departamento que se hayan adherido a la PSI. Deberán tener, al menos, rango de Subdirector/a General o equivalente, y serán designados por las personas de dichos organismos públicos que ostenten cargos con competencias específicas en cuanto a la organización general o de regulación de servicios comunes, o por sus órganos superiores.

iii) La persona titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones. Actuará, además, como Secretario/a, poniendo en conocimiento de los vocales las convocatorias acordadas por la Presidencia, preparando el orden del día, y ejecutando las decisiones del Comité que le correspondan.

3. Régimen de suplencias de los miembros del CDSI: En caso de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención o recusación y, en general, cuando concurra alguna causa justificada, se establece el siguiente régimen de suplencias de los miembros del CDSI:

a) El Presidente/a será sustituido por el Vicepresidente/a.

b) Los Vocales serán sustituidos por sus suplentes, que deberán ser funcionarios pertenecientes al grupo A1, con nivel 28 o superior, y serán nombrados por el mismo procedimiento que los titulares.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

c) El Secretario/a podrá ser sustituido por otro funcionario, con nivel 26 o superior, que será nombrado por la Presidencia.

4. El CDSI ejercerá las siguientes funciones:

a) Aprobar las propuestas de modificación y actualización permanente que se hagan sobre la PSI.
b) Velar por el cumplimiento de la PSI e impulsar su desarrollo y cumplimiento normativo.
c) Promover la mejora continua en la gestión de la seguridad de la información.
d) Resolver los conflictos de competencia en materia de seguridad de la información que pudieran aparecer entre los diferentes centros directivos.
e) Ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas. En este sentido, también podrá definir la planificación de estas actuaciones, que en todo caso deberán ser regulares.
f) Proveer los recursos y medios necesarios para asegurar la concienciación y formación en materia de seguridad de la información de todo el personal afectado por esta orden.
g) Evaluación y seguimiento de las decisiones tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.
h) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.
i) Aprobación de las normas de segundo y tercer nivel a las que se refiere el artículo 16.
j) Aprobar los planes de mejora de la seguridad en su ámbito de competencias, de conformidad con las disposiciones presupuestarias.
k) Revisión y aprobación anual del Proceso de Gestión de Riesgos especificado en el artículo 15.2.

5. Funcionamiento del CDSI.

Las sesiones del CDSI se considerarán debidamente constituidas, cuando asistan a sus reuniones al menos cuatro Vocales, el Presidente/a y el Secretario/a.

Asimismo, cabe la posibilidad de utilizar medios electrónicos para el funcionamiento del CDSI, de acuerdo con lo dispuesto en el artículo 17 de la Ley 40/2015, de 1 de octubre, que señala que los órganos colegiados se podrán constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas tanto de forma presencial como a distancia.

El CDSI se apoyará en el Grupo de Trabajo Técnico para la Seguridad de la Información, tanto para la preparación de los documentos que deban ser estudiados y aprobados por ella, como para el análisis o valoración de los expedientes para los que así estime conveniente. Además, el CDSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

El CDSI arbitrará los mecanismos que se estimen más adecuados para garantizar la coordinación con otros órganos colegiados del Departamento, especialmente, con la Comisión Ministerial de Administración Digital, regulada mediante la Orden ECE/91/2019, de 31 de enero, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Economía y Empresa y se regula su composición y funciones.

El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente/a.

6. El CDSI se regirá por las normas de funcionamiento previstas en la presente orden y, en lo no contemplado en ellas, por las normas previstas para los órganos colegiados en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

Artículo 8. *Grupo de Trabajo Técnico de Seguridad de la Información.*

1. Los órganos con competencias en materia de gestión de tecnologías de la información constituirán un Grupo de Trabajo Técnico para la Seguridad de la Información (en adelante, GTTSI).

2. El GTTSI colaborará con el CDSI en las cuestiones que éste le encomiende y en particular ejercerá las siguientes funciones, que podrán ser ampliadas dentro su ámbito competencial:

a) Elaboración de las propuestas de normas de segundo y tercer nivel a las que se refiere el artículo 16, y elevación de las mismas al CDSI para su aprobación.

b) Informar al CDSI sobre el cumplimiento de las normas de segundo nivel, y apoyar e impulsar el desarrollo del segundo y tercer nivel normativo.

c) Elaboración de los documentos que describan la responsabilidad de cada puesto, detallados de acuerdo a la normativa en vigor en materia de seguridad y privacidad, y elevación de los mismos al CDSI para su aprobación.

d) Elaboración de los planes de mejora de la seguridad, de conformidad con las disponibilidades presupuestarias, y su elevación al CDSI para su aprobación.

e) Informar al CDSI sobre el estado de las principales variables de seguridad de sus sistemas de información, y elaboración de un perfil general del estado de seguridad del Ministerio.

f) Promover la mejora continua en la gestión de la seguridad de la información en su ámbito de competencias.

g) Impulsar la formación y concienciación en materia de seguridad en su ámbito de competencias, y elevar al CDSI propuestas en cuanto a planes e iniciativas de formación.

h) Elaborar y elevar al CDSI aquellos informes que le sean requeridos, en materia de seguridad de la información.

3. El GTTSI estará compuesto por los siguientes miembros:

a) Presidente/a: Persona titular de la Subdirección General de Tecnologías de la Información y las Comunicaciones dependiente de la Subsecretaría del Ministerio de Asuntos Económicos y Transformación Digital.

b) Los Responsables de la Seguridad, de acuerdo con la definición del artículo 9.

c) Secretario/a: Responsable de la Seguridad de la Subdirección General de Tecnologías de la Información y las Comunicaciones dependiente de la Subsecretaría del Ministerio de Asuntos Económicos y Transformación Digital.

4. En las reuniones del GTTSI podrán participar cuantos asesores, internos o externos, estimen necesarios los miembros del mismo.

5. El Delegado de Protección de Datos participará, con voz, pero sin voto, en las reuniones del GTTSI. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

Artículo 9. *Responsables de la Seguridad.*

1. En base a lo dispuesto en el artículo 13.2.c) del Real Decreto 311/2022, de 3 de mayo, 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.

2. El ámbito de actuación de los Responsables de la Seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del centro o centros para los que haya sido designado Responsable de la Seguridad.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

3. Serán funciones del Responsable de la Seguridad, entre otras, las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Colaborar en el ámbito del GTTSI, en la elaboración la normativa de seguridad de segundo y tercer nivel definida en el artículo 16.
c) Velar por el cumplimiento del cuerpo normativo definido en el artículo 16.
d) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.
e) Promover la mejora continua en la gestión de la seguridad de la información.
f) Impulsar la formación y concienciación en materia de seguridad de la información.
g) Analizar los informes de autoevaluación y auditoría de la seguridad de la información.
h) Identificar las categorías de seguridad de los sistemas de información, así como determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
i) Realizar los análisis de riesgos en su ámbito de actuación, así como interpretar las medidas de seguridad del Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ampliándolas o sustituyéndolas, en base a lo dispuesto en el artículo 28 del Real Decreto 311/2022, de 3 de mayo, y firmar de la Declaración de Aplicabilidad.
j) En los procesos de Gestión de Cambios, el Responsable de la Seguridad deberá aprobar explícitamente aquellos cambios que impliquen un riesgo de nivel ALTO, en base a los dispuesto en el Anexo II del Real Decreto 311/2022, de 3 de mayo.
k) Obtener las certificaciones exigibles a la figura de los Responsables de la Seguridad, en base a lo dispuesto en el artículo 13.4 del Real Decreto 311/2022, de 3 de mayo.
l) Supervisar la implantación de las medidas de seguridad.
m) Cualquier otra función en el ámbito de la seguridad de la información y los servicios.

4. Existirá al menos un Responsable de la Seguridad en cada órgano superior o directivo del Ministerio con competencias de gestión de tecnologías de la información, según el Real Decreto 403/2020, de 25 de febrero, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 2, les sea de aplicación la presente PSI.
5. Los Responsables de Seguridad se designarán por la persona titular del órgano superior o directivo correspondiente, tendrán un nivel administrativo de nivel 28 o superior, y se atenderá al principio de diferenciación de responsabilidades establecido en el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo.

Artículo 10. *Responsables de la Información.*

1. De acuerdo con lo previsto en el artículo 13.2.a) del Real Decreto 311/2022, de 3 de mayo, los Responsables de la Información determinarán los requisitos de la información tratada, siendo los responsables últimos de su uso y acceso y, por lo tanto, de su mantenimiento y protección.
2. Dentro de las funciones de los Responsables de la Información, se encuentran las siguientes:

a) Aprobar, dentro de su ámbito de actuación y competencias, los requisitos en materia de seguridad de la información tratada.
b) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información. Para ello, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

c) Colaborar, junto a los Responsables del Servicio, y contando con la participación del Responsable de la Seguridad, en la realización de los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

d) Son los responsables de aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

e) Cualquier otra función en el ámbito de la seguridad de la información.

3. A los efectos previstos en el RGPD, y en la medida en que sea el que determine, solo o junto con otros, los fines y medios del correspondiente tratamiento de datos personales, los Responsables de la Información podrán tener la consideración de responsables o encargados del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación. Cuando se de esta circunstancia, los Responsables de la Información deberán mantener los registros de las actividades de tratamiento a los que se refiere el artículo 30 del RGPD.

4. Existirá al menos un Responsable de la Información en cada órgano superior o directivo del Ministerio con competencias de gestión de tecnologías de la información, según el Real Decreto 403/2020, de 25 de febrero, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 2, les sea de aplicación la presente PSI.

5. Los Responsables de la Información se designarán por la persona titular del órgano superior o directivo correspondiente, y tendrán un nivel administrativo 28 o superior.

Artículo 11. *Responsables del Servicio.*

1. De acuerdo con lo previsto en el artículo 13.2.b) del Real Decreto 311/2022, de 3 de mayo, los Responsables del Servicio determinan los requisitos de los servicios prestados, y tienen la responsabilidad última del uso que se haga de un servicio basado en tecnologías de la información y, por tanto, de su protección.

2. Dentro de las funciones de los Responsables del Servicio recaen las siguientes:

a) Aprobar, dentro de su ámbito de actuación y competencias, los requisitos en materia de seguridad de los servicios prestados.

b) Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio. Para ello, el Responsable del Servicio solicitará informe del Responsable de la Seguridad.

c) Colaborar, junto a los Responsables de la Información, y contando con la participación del Responsable de la Seguridad, en la realización de los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

d) Son los responsables de aceptar los riesgos residuales respecto de los servicios calculados en el análisis de riesgos.

e) Cualquier otra función en el ámbito de la seguridad de los servicios prestados.

3. Existirá al menos un Responsable del Servicio en cada órgano superior o directivo del Ministerio con competencias de gestión de tecnologías de la información, según el Real Decreto 403/2020, de 25 de febrero, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 2, les sea de aplicación la presente PSI.

4. Los Responsables del Servicio se designarán por la persona titular del órgano superior o directivo correspondiente, y tendrán un nivel administrativo 28 o superior.

Artículo 12. *Responsables del Sistema.*

1. De acuerdo con lo previsto en el artículo 13.2.d) del Real Decreto 311/2022, de 3 de mayo, los Responsables del Sistema, se encargarán 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.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

2. Dentro de sus funciones se encuentran las siguientes:

a) Definir la tipología y sistemas de gestión de los sistemas de información, estableciendo los criterios de uso y los servicios disponibles en éste.
b) Cerciorarse de que las medidas de seguridad se integran adecuadamente dentro del marco tecnológico y de seguridad del Departamento.
c) Adoptar las medidas correctoras adecuadas de acuerdo a las evaluaciones y auditorías de seguridad.
d) Acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
e) Garantizar que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.
f) Cualquier otra función en el ámbito de la seguridad de sistemas de información que le sea encomendada a través de la normativa de seguridad.

3. Existirá un Responsable del Sistema en cada órgano superior o directivo del Ministerio con competencias de gestión de tecnologías de la información, según el Real Decreto 403/2020, de 25 de febrero, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 2, les sea de aplicación la presente PSI.
4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el titular del órgano directivo podrá designar los Responsables de Sistema delegados que considere necesarios entre los funcionarios de carrera del órgano directivo, que tendrán dependencia funcional directa del Responsable del Sistema y serán responsables en su ámbito de todas aquellas acciones que les delegue.
5. Los Responsables del Sistema se designarán por la persona titular del órgano superior o directivo correspondiente, tendrán un nivel administrativo de nivel 28 o superior, salvo en el caso de Responsables de Sistema delegados, que podrán tener cualquier nivel administrativo. En cuanto a la designación de los Responsables del Sistema y sus delegados, se atenderá al principio de diferenciación de responsabilidades establecido en el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo.

Artículo 13. *Delegado de Protección de Datos.*

1. En el ámbito de los tratamientos de datos personales, y sin perjuicio de las atribuciones establecidas en el RGPD de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de los Responsables de la Seguridad, el Delegado de Protección de Datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma, y en particular:

2. El Delegado de Protección de Datos prestará asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto, serán responsabilidad de los respectivos responsables del tratamiento.
3. Ejercerá labores de asistencia y asesoramiento a los responsables del tratamiento de datos personales, a los Responsables de la Seguridad y a los responsables del Sistema, en los procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad.
4. Prestará asesoramiento a los Responsables de la Seguridad y a los Responsables del Sistema, en cuanto a la implantación de medidas de seguridad que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.

Artículo 14. *Grupos de trabajo.*

El CDSI podrá articular la creación de grupos de trabajo para la realización de actividades tales como la elaboración de estudios, trabajos e informes, que se estimen convenientes.

Artículo 15. *Gestión de los Riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos, vigilancia continua y reevaluación periódica, previstos en los artículos 7 y 10 del Real Decreto 311/2022, de 3 de mayo.
2. El Proceso de Gestión de Riesgos, que comprende la definición de las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el CDSI. El Proceso de Gestión de Riesgos aprobado conformará la guía metodológica básica para la elaboración de los respectivos análisis de riesgos, y por lo tanto facilitará la homogenización y comparación de los resultados de cada uno de los análisis de riesgos que se realicen.
3. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.
4. Cada órgano superior o directivo del Ministerio de Asuntos Económicos y Transformación Digital, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que conforme al artículo 2 les sea de aplicación la presente PSI dentro de sus respectivos ámbitos de actuación y competencias, solicitarán a los Responsables de la Seguridad el preceptivo análisis de riesgos para que se proponga el tratamiento adecuado, calculando los riesgos residuales, identificando carencias y debilidades.
5. Los Responsables de la Seguridad serán los encargados de realizar el análisis de riesgos en tiempo y forma, contando con la colaboración de los correspondientes Responsables del Servicio y Responsables de la Información.
6. Tras la calificación de la información y la determinación del nivel de seguridad del sistema por parte de los Responsables de la Información y los Responsables de Sistemas, se obtendrá la matriz de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio. La evaluación de los riesgos se realizará identificando los riesgos residuales y, con base en ellos, se determinará el Plan de Tratamiento de Riesgos.
7. Será responsabilidad de los Responsables del Servicio y de los Responsables de la Información, la aceptación de los riesgos residuales y el impulso de la ejecución de auditorías de seguridad, las cuales deberán ejecutarse en base a la planificación que determine el CDSI.
8. En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo 17, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del Delegado de Protección de Datos, se puedan añadir a los establecidos conforme al Real Decreto 311/2022, de 3 de mayo, si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales fuesen de alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de Protección de Datos (AEPD). En este aspecto,

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD.

Artículo 16. *Estructura normativa.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior:

a) Primer nivel normativo: Está constituido por la PSI. Además incluye la normativa y disposiciones generales en materia de seguridad aplicables a los órganos y organismos a los que conforme al artículo 2, les sea de aplicación la presente PSI, como pueden ser el Real Decreto 311/2022, de 3 de mayo, el RGPD, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las disposiciones generales de la Secretaría General de Administración Digital, u otras, que en materia de seguridad de la información sean emitidas por un organismo competente. También incluye las disposiciones y normativa de carácter general sobre la seguridad de los sistemas de información que gestionen información clasificada.

b) Segundo nivel normativo: Constituido por las resoluciones de seguridad que se definan en cada ámbito organizativo de aplicación específico. Las resoluciones, que comprenderán los procedimientos, las normas, las instrucciones técnicas de seguridad, y recomendaciones de seguridad, serán de obligado cumplimiento. Se aprobarán en el ámbito de cada uno de los órganos y organismos a los que, conforme al artículo 2, sea de aplicación la presente PSI, y su cuerpo documental deberá estar disponible para su consulta general en la red interna del correspondiente órgano u organismo. En el ámbito del Ministerio serán aprobadas por la persona titular de la Subsecretaría de Asuntos Económicos y Transformación Digital. En el resto de órganos y organismos serán aprobadas por las personas que ostenten cargos con competencias específicas en cuanto a la regulación de la seguridad, y en su defecto, en organización general o de regulación de servicios comunes.

c) Tercer nivel normativo. Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Se consideran incluidas en este nivel normativo:

i) Las guías de seguridad de las tecnologías de la información y la comunicación elaboradas por el Centro Criptológico Nacional (guías CCN-STIC).

ii) Las normas o recomendaciones aprobadas por órganos y organismos con competencias regulatorias en materia de seguridad o de protección de datos, como son el Centro Criptológico Nacional, la Secretaría de Estado de Digitalización e Inteligencia Artificial, la Secretaría General de Administración Digital, o la AEPD.

iii) Conjunto de procedimientos técnicos elaborados y aprobados por los Responsables de Seguridad en sus ámbitos de actuación.

iv) Recomendaciones, guías de configuración y buenas prácticas publicadas por organismos u organizaciones internacionales y por los fabricantes de productos de seguridad.

2. Además de la normativa enunciada en el apartado 1, la estructura normativa podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a la presente PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como estándares de seguridad, buenas prácticas, o informes técnicos.

3. El personal de cada uno de los órganos u organismos adscritos a la presente PSI tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. El CDSI establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

5. Este marco normativo estará a disposición del personal del Ministerio de Asuntos Económicos y Transformación Digital, y del de aquellos organismos públicos y entidades de derecho público vinculados o dependientes del Departamento que formen parte del ámbito de aplicación de la PSI.

Artículo 17. *Protección de datos de carácter personal.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Asuntos Económicos y Transformación Digital, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre.

2. Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

3. En particular, se tendrá en cuenta el artículo 32 del RGPD, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación a los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas.

4. Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos Responsables de los Sistemas, podrán implementar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto que la protección de los datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, y teniendo en cuenta, entre otros, los principios de limitación de finalidad; prohibición del tratamiento de los datos personales para fines distintos; el principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.

Artículo 18. *Terceras partes.*

1. Cuando el Ministerio de Asuntos Económicos y Transformación Digital utilice servicios o maneje información de otros organismos, se les hará partícipes de esta PSI, se establecerán canales de información y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

2. Cuando el Ministerio de Asuntos Económicos y Transformación Digital preste servicios o ceda información a terceros, se les hará partícipes de esta PSI y de la Normativa de Seguridad que ataña a dichos servicios e información. Los mismos quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad.

3. Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, se requerirá un informe del Responsable de la Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho

cve: BOE-A-2023-8109
Verificable en https://www.boe.es

informe habrá de ser aprobado por los responsables de la información y los servicios afectados.

Artículo 19. *Concienciación y formación.*

1. Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información.
2. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Ministerio de Asuntos Económicos y Transformación Digital, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización.

Disposición adicional primera. *Actualización permanente de la Política de Seguridad de la Información.*

La presente orden deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Digital a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad. Las propuestas de las sucesivas revisiones corresponden al CDSI, de conformidad con el artículo 7.

Disposición adicional segunda. *No incremento del gasto público.*

La aplicación de esta orden no conllevará incremento del gasto público. Las medidas incluidas en la presente orden no supondrán incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición derogatoria única. *Derogación normativa.*

Se derogan cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta orden, y en particular en aquellas materias del ámbito competencial del Ministerio de Asuntos Económicos y Transformación Digital.

Disposición final primera. *Publicidad de la Política de Seguridad de la Información.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital y sus sedes asociadas.

Disposición final segunda. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 16 de marzo de 2023.–La Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño Santamaría.

cve: BOE-A-2023-8109
Verificable en https://www.boe.es