III. OTRAS DISPOSICIONES

MINISTERIO DE JUSTICIA

13423 *Orden JUS/564/2023, de 30 de mayo, por la que se aprueba la Política de Seguridad del Ministerio de Justicia.*

Una visión integral de la organización de la seguridad permitirá dar cumplimiento a los diferentes marcos de regulación y a sus propios bienes jurídicos protegidos, de una manera uniforme, eficaz y con el uso eficiente de sus recursos.

La organización de la seguridad del Ministerio de Justicia debe adaptarse a diversos contextos normativos que le son aplicables, principalmente los relativos a la administración electrónica, administración judicial electrónica, protección de datos personales e información clasificada, con el Esquema Nacional de Seguridad como marco común de medidas técnicas y organizativas, sin perjuicio de las especialidades en cada ámbito.

Los marcos normativos aplicables a este Ministerio, requieren del desarrollo de sus principios y requisitos, la definición de roles, responsabilidades, órganos de gobierno y funciones que reflejan el desarrollo del gobierno de la seguridad, con las facultades de dirección estratégica y su supervisión, y la convergencia de las diferentes esferas de seguridad, como la protección de bienes físicos, personas, servicios de información y activos tecnológicos de soporte, información clasificada, datos personales, e incluso en un sentido más amplio, la protección del medio ambiente, la economía, la vida humana y la confianza de la población en la capacidad de las Administraciones públicas.

La suma de gobierno de seguridad y convergencia de esferas responde a la creciente complejidad de los riesgos, que por un lado, cada vez más provienen de la fusión o encadenamiento de tipos de amenazas, en forma de ataques híbridos o combinados que se valen de técnicas que combinan distintas vulnerabilidades, incluso de diferentes esferas de seguridad, y por otro, impactan sobre una malla cada vez más interconectada de consecuencias que afectan a más de un factor a proteger (bien físico, servicio esencial, vida humana, medio ambiente, datos personales, etc.).

Con esta visión integral de la seguridad se supera el alcance de la Política de Seguridad de la Información en el ámbito de la administración electrónica de 2017, limitado principalmente a este ámbito, y que es también objeto de esta nueva política de seguridad, como administración pública sujeta a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de las relaciones entre la Administración Pública y los ciudadanos a través de los medios electrónicos, estableciendo los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada y los servicios prestados.

Por otro lado, esta nueva política recoge y se adapta a las novedades normativas posteriores a 2017, como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 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. En este nuevo marco normativo se evoluciona de un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos. En el ámbito de la seguridad del tratamiento del 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

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), serán de aplicación las medidas de seguridad que correspondan del Esquema Nacional de Seguridad, de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de medidas de seguridad en el ámbito del sector público, y el artículo 37 de la Ley Orgánica 7/2021, de 26 de mayo

La presente orden cumple con los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. Así, atiende a la necesidad de aprobar la Política de Seguridad del Ministerio de Justicia.

Además, constituye y forma parte de la misma, la Política de Seguridad de la Información del Ministerio de Justicia, por ser éste, uno de los ámbitos objeto de aquélla, y con ello, da cumplimiento al mandato contenido en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo. Además, es eficaz y proporcionada en el cumplimiento de este propósito sin afectar en forma alguna a los derechos y deberes de la ciudadanía. También contribuye a dotar de mayor seguridad jurídica a la organización y funcionamiento de la Administración General del Estado, en lo que se refiere al Ministerio de Justicia. Cumple también con el principio de transparencia, ya que identifica claramente su propósito, aunque al tratarse de una norma puramente organizativa, su tramitación no ha requerido de la consulta pública previa y de los trámites de audiencia e información pública. No obstante, su memoria ofrece una explicación completa de su contenido. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

Se ha recabado informe de la Comisión Ministerial de Administración Digital del Ministerio de Justicia y de la Agencia Española de Protección de Datos.

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

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de la presente orden la aprobación de la Política de Seguridad (en adelante, PS) en los ámbitos de la Administración Electrónica, Protección de datos personales y Protección de la información clasificada del Ministerio de Justicia, así como del marco organizativo y tecnológico de la misma.

2. La PS será de obligado cumplimiento para todos los órganos y unidades que conforman la estructura del Ministerio de Justicia y para todo el personal que realice tratamiento de información de la que sea responsable el Ministerio de Justicia con independencia de su destino, condición laboral o relación por la que proceda al tratamiento.

3. La PS afectará a la información tratada por medios electrónicos y a la información en soporte papel que el Ministerio gestiona en el ámbito de sus competencias. La taxonomía de la información se define según las siguientes normas:

a) Tendrá carácter de información clasificada la que esté dentro del ámbito regulado en la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

b) La información que contenga datos de carácter personal se verá afectada por 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, RGPD), por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, en su caso, por 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, y demás disposiciones generales o especiales reguladoras de la materia.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

c) La información contenida en los sistemas de información en el ámbito de la administración electrónica queda regulada por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

d) La información producida, conservada o reunida, cualquiera que sea su soporte, susceptible de formar parte del patrimonio documental se verá afectada por el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

e) La información de gestión interna es aquella que no se produce como resultado de la función administrativa, aunque sea necesario disponer de ella para el correcto desarrollo de las competencias del Ministerio, como copias o duplicados de documentos originales que estén localizados y en buen estado de conservación, borradores o primeras versiones de documentos, publicaciones oficiales, ejemplares de ediciones, catálogos y publicaciones comerciales, el acceso al contenido de carpetas compartidas y el resto de información de apoyo que gestione el Departamento. A efectos de seguridad, confidencialidad y deber de secreto profesional, la información de gestión interna podrá ser calificada como protegida.

4. Se podrán adscribir a la presente PS aquellos organismos públicos dependientes del Ministerio de Justicia que no tengan establecida su propia política de seguridad y así lo soliciten.

5. Respecto de los sistemas de información prestados y gestionados por el Ministerio de Justicia para la Administración de Justicia, y sometidos a la Política de Seguridad de la Información de la Administración Judicial Electrónica, se asignan dentro de la estructura organizativa aquí regulada, determinadas funciones que permitan dar cumplimiento a la citada política de seguridad.

Artículo 2. *Misión.*

En materia tecnológica el Ministerio de Justicia, en su ámbito competencial, presta y pone a disposición de los órganos y oficinas judiciales y fiscales los servicios y sistemas de Tecnologías de la Información y Comunicaciones (TIC) para el desarrollo de sus funciones.

Asimismo, los servicios TIC del Ministerio de Justicia garantizan las relaciones electrónicas de los ciudadanos y profesionales con la Administración de Justicia, y con el Ministerio de Justicia.

Por último, estos servicios pueden ser prestados a otras Comunidades Autónomas con competencias en materia de Justicia, así como a otras administraciones y entidades públicas.

Artículo 3. *Principios de seguridad.*

El Ministerio de Justicia tratará la información y los datos personales bajo su responsabilidad conforme a los principios y requisitos recogidos en los diferentes marcos normativos indicados en el artículo 1 que serán desarrollados e implementados a través de la presente PS y su desarrollo normativo.

Artículo 4. *Estructura organizativa.*

1. La estructura organizativa para la gestión de la seguridad en los ámbitos descritos por la PS del Ministerio de Justicia está compuesta por los siguientes órganos y agentes:

a) El Comité de Gobierno de Seguridad y Riesgos.
b) El Comité de Ciberseguridad.
c) El Grupo de Coordinación de Protección de Datos.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

d) El Servicio de Protección de Información Clasificada.
e) Los Responsables de Seguridad de la Información.
f) Los Responsables de la Información.
g) Los Responsables del Servicio.
h) Los Responsables del Sistema.
i) Los Responsables del Tratamiento.
j) Los Encargados del Tratamiento.
k) Los Delegados de Protección de Datos.
l) El Jefe de Seguridad del Servicio de Protección de Información Clasificada.

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por la presente orden, la PS del Ministerio de Justicia.

Artículo 5. *El Comité de Gobierno de Seguridad y Riesgos.*

1. Adscrito a la Subsecretaría, se crea el Comité de Gobierno de Seguridad y Riesgos (en adelante, CGSR), como órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará todas las actividades relacionadas con la seguridad del Ministerio de Justicia.
2. El CGSR estará integrado por los siguientes miembros:

a) Presidente: La persona titular de la Subsecretaría de Justicia. Tendrá voto de calidad en la toma de decisiones del Comité. En caso de ausencia, vacante o enfermedad será sustituido por el Vicepresidente, y, en su defecto, por el miembro del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden.
b) Vicepresidente: La persona titular de la Dirección General de Transformación Digital (DGTDAJ).
c) Vocales: Un representante propuesto por el titular de cada uno de los siguientes órganos u organismos del Departamento, que serán designados por la persona titular de la Subsecretaría de Justicia, entre funcionarios con nivel mínimo de Subdirector General o asimilados:

1.º Secretaría de Estado de Justicia.
2.º Abogacía General del Estado.
3.º Dirección General de Transformación Digital.
4.º Centro de Estudios Jurídicos (CEJ).
5.º Mutualidad General Judicial (MUGEJU).

Asimismo, serán Vocales del Comité, el Responsable de Seguridad de la División de Oficialía, los Responsables de Seguridad de la Información, el Jefe de Seguridad del Servicio de Protección de Información Clasificada del Ministerio de Justicia y, con voz, pero sin voto, el Delegado de Protección de Datos de la Subsecretaría de Justicia.
En caso de vacante, ausencia o enfermedad y en general cuando concurra una causa justificada, el Vicepresidente designará sustituto con nivel de Subdirector General entre los funcionarios de su Dirección General y los Vocales podrán ser sustituidos por suplentes de tales órganos que reúnan las mismas condiciones, designados por el mismo procedimiento que los titulares.
d) Secretario: Será un funcionario de la Oficina de Seguridad, que no tendrá voto y que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar y elaborará el borrador del acta de la sesión.

Además del Delegado de Protección de Datos que participa como Vocal, el Grupo de Coordinación de la Protección de Datos en el Ministerio de Justicia designará al delegado o delegados que deban asistir en función de la materia a tratar en cada convocatoria y su ámbito de competencias. Asistirán con voz, pero sin voto.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

El Presidente del Comité podrá autorizar la asistencia a las reuniones de expertos en las materias que se vayan a tratar, que tendrán el carácter de asesores, participando con voz, pero sin voto.

3. El CGSR ejercerá las siguientes funciones:

a) Garantizar la definición e implantación de la presente política de seguridad integral.

b) Garantizar la identificación de escenarios de riesgos, y determinar los límites de tolerancia para evitar aquellos de alto riesgo.

c) Seguir el correcto desarrollo de los planes de contingencia en caso de materialización de los escenarios.

d) Fomentar una cultura corporativa de riesgos.

e) Recibir y evaluar la información de los comités y grupos subordinados en torno a riesgos, y de todas las áreas de la organización, sobre los peligros que enfrentan.

f) Garantizar la revisión activa de los límites de exposición a las amenazas.

g) Supervisar las acciones de prevención y el cumplimiento de sus objetivos.

h) Procurar que la visión, la misión y los objetivos estratégicos del Ministerio sean afines a las medidas dispuestas para mitigar eventuales contingencias.

i) Elaborar y elevar las propuestas de modificación y actualización permanente de la PS del Ministerio de Justicia.

j) Aprobar las normas de desarrollo de la PS de primer nivel.

k) Definir y asignar los roles en los distintos ámbitos de seguridad, en base a criterios de garantía en lo relativo a la segregación de tareas, y en cumplimiento de las normativas de Protección de Información Clasificada, Administración Electrónica, Esquema Nacional de Seguridad y cualquier otra norma o necesidad del Ministerio de Justicia que requiera la designación para el desarrollo de una función relacionada con la seguridad.

4. El CGSR se reunirá con carácter ordinario al menos una vez al año y con carácter extraordinario cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo no previsto en la presente orden, por lo dispuesto en el capítulo II, sección 3.ª, del título preliminar de la Ley 40/2015, de 1 de octubre, ya citada, que regula el funcionamiento de los órganos colegiados de la Administración.

Las sesiones podrán serán grabadas con objeto de confeccionar el acta de las reuniones, y de resolver las posibles impugnaciones antes de su aprobación.

5. El CGSR podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 6. *Comité de Ciberseguridad.*

1. Adscrito a la Dirección General de Transformación Digital de la Administración de Justicia, se crea el Comité de Ciberseguridad (CC), como órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dependiente de la Dirección General de Transformación Digital de la Administración de Justicia.

El CC estará compuesto por:

a) Presidente: La persona titular de la DGTDAJ.

b) Vocales: Los Vocales, que podrán ser permanentes o no permanentes, serán las personas designadas por la persona titular de la DGTDAJ a propuesta de los titulares de los siguientes órganos, organismos, unidades y cargos del Departamento, entre funcionarios con nivel mínimo de Subdirector General o asimilados:

Vocales Permanentes:

1.º Subdirección General de Impulso e Innovación de los Servicios Digitales de Justicia.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

2.º Subdirección General de Calidad de los Servicios Digitales, Ciberseguridad y Operaciones.
3.º División de Servicios Digitales Departamentales.
4.º Unidades TIC de las organizaciones de Abogacía General del Estado, MUGEJU y CEJ.
5.º Responsables de Seguridad de la Información.
Vocales no Permanentes:

1.º Titulares de los órganos directivos, y organismos adscritos a la PS, como responsables de la información, servicios o tratamiento de datos.
2.º Delegados de protección de datos.
3.º Jefe de Seguridad del Servicio de Protección de Información Clasificada

c) Secretario: Será un funcionario de la Oficina de Seguridad, que no tendrá voto y que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.

2. Será necesaria la asistencia de los vocales no permanentes del Comité y serán convocados a las reuniones, si en razón de los asuntos objeto de cada convocatoria, les afecte a su ámbito de competencias o funciones, como responsables de la información, servicios o protección de datos. Los vocales permanentes y no permanentes tendrán derecho de voz y voto.
3. Los delegados de protección de datos serán convocados si el objeto de los asuntos a tratar afecta a la materia de protección de datos que requiera de su asesoramiento o supervisión. Serán convocados aquellos delegados en función del ámbito de aplicación de los asuntos a tratar a través del Grupo de Coordinación para la Protección de Datos en el Ministerio de Justicia.
4. En las reuniones del CC podrán participar, con voz, pero sin voto, cuantos asesores, internos o externos, estimen necesarios los miembros convocados del mismo.
5. El CC ejercerá las siguientes funciones:

a) Elaborar y elevar al CGSR las propuestas de modificación y actualización permanente de la PS del Ministerio de Justicia.
b) Impulsar el cumplimiento de la PS y su desarrollo normativo.
c) Proponer y elevar para su aprobación por el CGSR las normas de desarrollo de primer nivel de la PS, según lo previsto en el artículo 21.
d) Aprobar las normas de desarrollo de la PS de segundo y tercer nivel. Estas funciones será competencia de los miembros y Vocales Permanentes.
e) Aprobar los riesgos residuales de los sistemas de información que resulten elevados.
f) Aprobar los niveles de riesgos y los riesgos residuales de los sistemas de la Administración de Justicia, mientras no se decida en la Política de Seguridad de la Información de la Administración Judicial Electrónica su aprobación por los responsables de la información, de los servicios y tratamiento de datos, de los órganos y oficinas judiciales y fiscales.
En caso de designación de los responsables indicados serán convocados a las reuniones de esta materia, quedando la misma excluida de votación y sometida a la decisión de los citados responsables.
g) Aprobar la normativa de desarrollo de la Política de Seguridad de la Información de la Administración Judicial Electrónica, aplicables exclusivamente en el ámbito de competencias del Ministerio de Justicia, sin perjuicio de otras aprobaciones que establezca su política de seguridad y de las instrucciones que deban dictarse por las diferentes instituciones, órganos y organismos respecto de cada colectivo de usuarios.
h) Velar por la difusión de la PS, promoviendo actividades de concienciación y formación en materia de seguridad.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

i) Apoyar la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de Seguridad de la Información a través de los órganos que se creen al respecto en las Administraciones Públicas.

j) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento.

k) Promover la mejora continua en la gestión de la seguridad de la información.

l) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por los Responsables de Seguridad de la información.

m) Resolver los conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información.

n) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PS y su normativa de desarrollo.

6. El CC se reunirá con carácter ordinario mensualmente, y con carácter extraordinario cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo no previsto en la presente orden, por lo dispuesto en el capítulo II, sección 3.ª, del título preliminar de la Ley 40/2015, de 1 de octubre, ya citada, que regula el funcionamiento de los órganos colegiados de la Administración.

Las sesiones podrán ser grabadas con objeto de confeccionar el acta de las reuniones, y de resolver las posibles impugnaciones antes de su aprobación.

7. El CC podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 7. *Grupo de Coordinación de Protección de Datos.*

Dentro de la estructura organizativa de la presente PS, forma parte el Grupo de Coordinación de Protección de Datos, creado de conformidad con la Instrucción 7/2020, de 21 de diciembre, de la Subsecretaría de Justicia, que designarán entre sus miembros a los asistentes a las reuniones de los diferentes órganos recogidos en el presente orden ministerial.

Artículo 8. *Servicio de Protección de Información Clasificada.*

En cumplimiento de las normas de la Autoridad Nacional para la Protección de la Información Clasificada, el Ministerio debe designar un Jefe de Seguridad para cada servicio de protección (Jefe de Seguridad del Servicio de Protección de Información Clasificada o JSSP).

Corresponde al JSSP organizar, dirigir y controlar un determinado servicio de protección, así como cumplir y hacer cumplir la normativa vigente. Sus cometidos se encuentran definidos en el apartado 5.4 de la norma NS/01 sobre estructura nacional de protección de la información clasificada, que a alto nivel son:

a) Velar por la correcta protección de la información clasificada en su ámbito de responsabilidad.

b) Controlar la aplicación de todos los aspectos de las Normas de la Autoridad Nacional, en lo que concierne a la protección de la información clasificada bajo su servicio.

c) Proponer y aplicar las medidas específicas de seguridad propias dentro del Ministerio, relacionadas con la información clasificada bajo su servicio.

d) Estimular, mediante los correspondientes programas de formación, divulgación y de reciclaje, la sensibilidad en materia de seguridad del personal relacionado con la información clasificada.

La designación del Jefe de Seguridad del Servicio de Protección de Información Clasificada será efectuada por el CGSR a propuesta del titular de la DGTDAJ.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Artículo 9. *Los Responsables de Seguridad de la información.*

1. El Responsable de Seguridad de la información es el responsable de desarrollar e implementar el programa de seguridad de la información del Ministerio, que incluye procedimientos y políticas diseñados para proteger las comunicaciones, los sistemas y los activos de información de la organización de amenazas internas y externas dirigidas sobre vectores de ataque físicos y lógicos. Tomará las decisiones para satisfacer los requisitos de seguridad de la información, seguridad en el tratamiento de datos personales y de los servicios proporcionados por tecnologías de la información, atendiendo las directrices marcadas por el Comité de Gobierno de Seguridad y Riesgos.

Adicionalmente:

a) Representa al Ministerio de Justicia en foros nacionales e internacionales relacionados con seguridad de la información y riesgos tecnológicos.

b) Recolecta y revisa la información de los entornos de TI y la actividad del Ministerio de Justicia y organizaciones dependientes, para identificar los impactos potenciales de los riesgos de información y TI en los objetivos y las operaciones del Ministerio.

c) Identifica amenazas y vulnerabilidades potenciales relativas al personal, los procesos y la tecnología, para permitir el análisis de riesgos de información y TI.

d) Desarrolla un conjunto integral de escenarios de riesgos de TI, sobre la base del impacto potencial en los objetivos y las operaciones del Ministerio.

e) Propone las normas de desarrollo de la PS.

f) Establece y mantiene un registro de riesgos de TI, para ayudar a garantizar que los escenarios de riesgo identificados se tengan en cuenta y se incorporen al perfil de riesgos del Ministerio.

g) Colabora en el desarrollo de programas de concienciación y capacitación en seguridad de la información.

h) Propuesta de valoración de las dimensiones de seguridad, la determinación de la categoría de seguridad, elaboración del preceptivo análisis de riesgos, en materia de seguridad de la información y privacidad y, en su caso, la preceptiva evaluación de impacto de protección de datos, proponiendo el tratamiento adecuado una vez calculados los riesgos residuales, contando para ello con el asesoramiento y apoyo de los delegados de protección de datos. Elevar al CC aquellos análisis de riesgos y evaluaciones de impacto en protección de datos con un riesgo elevado, sin perjuicio de la decisión última del responsable del tratamiento.

i) La coordinación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad de la información.

j) El mantenimiento actualizado del marco documental de la seguridad en los ámbitos de aplicación de la presente PS.

k) La gestión de las incidencias de seguridad que se produzcan, informando a los responsables afectados, así como al Delegado de Protección de Datos en caso de violaciones de seguridad de los datos personales. El responsable de seguridad informará al CC las incidencias de seguridad más relevantes.

2. Los Responsables de Seguridad de la información serán designados por el Comité de Gobierno de Seguridad y Riesgos a propuesta del titular de la DGTDAJ, CEJ, MUGEJU.

3. El ámbito de actuación de cada Responsable de Seguridad de la información 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 órgano al que pertenezca dicho Responsable de Seguridad.

4. El Responsable de Seguridad de la información de la DGTDAJ representará al Ministerio de Justicia en el Subcomité de Seguridad del Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE), salvo que el Comité de Ciberseguridad decida otra designación.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Artículo 10. *Los Responsables de la Información y Responsables del Servicio.*

Los Responsables de la Información y los Responsables del Servicio, tienen la potestad, dentro de su ámbito de actuación, en virtud del principio de responsabilidad diferenciada, de establecer los requisitos de seguridad de la información tratada y de los servicios prestados, y, por lo tanto, de determinar los niveles de seguridad de la información y de los servicios, y aceptar los niveles de riesgo residuales que afecten a la información y a los servicios.

Si el sistema de información contiene datos personales las funciones anteriores serán llevadas a cabo por el responsable del tratamiento de dichos datos, con el asesoramiento del delegado de protección de datos asignado.

Las funciones del Responsable de la Información y del Responsable del Servicio recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

En el ámbito de la Administración de Justicia, o de otras entidades externas a las que se preste servicios tecnológicos, los responsables de la información serán designados por los órganos y entidades destinatarias de los sistemas de información, y de acuerdo con la Política de Seguridad de la Información de la Administración Judicial Electrónica. En su defecto, sus funciones recaerán en el Comité de Ciberseguridad.

Artículo 11. *Los Responsables del Sistema.*

1. 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.

El Responsable del Sistema tiene las siguientes funciones:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

2. Las unidades tecnológicas del Ministerio de Justicia asumen la responsabilidad del sistema, correspondiendo a sus titulares la máxima responsabilidad, y que podrán designar Responsables del Sistema Delegados.

Artículo 12. *Los Responsables del tratamiento.*

1. Cada órgano superior o directivo del Ministerio de Justicia, así como cada organismo público dependiente del Departamento, a los que les sea de aplicación la PS, designará al responsable del tratamiento.

2. Los responsables del tratamiento asumirán las obligaciones y responsabilidades establecidas en el marco normativo de protección de datos aplicable, contando con el asesoramiento de los delegados de protección de datos asignados.

Los órganos superiores o directivos del Ministerio de Justicia, así como cada organismo público dependiente del departamento, a los que les sea de aplicación la PS, ostentarán la condición de responsables del tratamiento por designación legal o por atribución de competencias.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Artículo 13. *Los Encargados del tratamiento.*

1. La persona designada como Encargado del tratamiento de datos personales es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta de la persona designada Responsable del tratamiento.

2. De conformidad con sus competencias, el Ministerio de Justicia, a través de la Dirección General de Transformación Digital de la Administración de Justicia, tendrá la consideración de «Encargado del Tratamiento» en el tratamiento de datos de carácter personal en las aplicaciones y servicios digitales diseñados, desarrollados o en mantenimiento por parte de la Dirección General de Transformación Digital y que hayan sido creados o implantados en el ámbito de competencias del Ministerio de Justicia, y puestos a disposición de Juzgados, Tribunales, Fiscalías, Oficinas Judicial y Fiscal, órganos técnicos auxiliares de la Administración de Justicia, unidades administrativas, órganos y organismos del departamento, así como de otras Administraciones, entidades e instituciones públicas en virtud de procedimientos de adhesión u otros instrumentos de la misma naturaleza previstos en la legislación vigente.

3. Esta misma condición de encargado del tratamiento será asumida por cualquier órgano, organismo, o unidad del Ministerio de Justicia que de acuerdo con sus competencias lleve o pueda llevar a cabo tratamiento de datos por cuenta de terceros.

4. La condición de Encargado del tratamiento supone la asunción de las obligaciones y responsabilidades establecidas para dicha figura en el marco normativo de protección de datos aplicable, contando con el asesoramiento de los delegados de protección de datos asignados, conforme a la disposición adicional séptima del Real Decreto 453/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Justicia, y se modifica el Reglamento del Servicio Jurídico del Estado, aprobado por el Real Decreto 997/2003, de 25 de julio.

5. Los delegados de protección de datos del Ministerio de Justicia que den servicio a los órganos, organismos, o unidades que tengan o adquieran la condición de encargados del tratamiento, asumirán las funciones que les corresponden de conformidad con el marco normativo aplicable como delegados de protección de datos del encargado.

Artículo 14. *Los Delegados de Protección de Datos.*

1. Las normas de desarrollo normativo de la presente política de seguridad establecerán los mecanismos de coordinación con los Delegados de Protección de Datos para que estos puedan informar, asesorar y supervisar sobre el cumplimiento de las diferentes obligaciones, por parte de los responsables o encargados de los tratamientos de datos personales, establecidas en el correspondiente marco normativo, garantizando la obligación del responsable y del encargado del tratamiento que el Delegado de Protección de Datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

Se garantizará su participación desde la etapa más temprana posible en todas las cuestiones relativas a la protección de los datos, y especialmente, y sin perjuicio de otras funciones, desde el propio diseño de los tratamientos, en el análisis y gestión de riesgos, en las evaluaciones de impacto, en la gestión de brechas de seguridad, auditorias, revisión y actualización del registro de actividades de tratamiento, ejercicio de derechos de los interesados y reclamaciones.

2. Sin perjuicio de su coordinación con los responsables de los tratamientos, y encargados, con objeto de garantizar participación efectiva de los Delegados de Protección de Datos en las cuestiones relativas a su ámbito de actuación, serán convocados, con voz pero sin voto, a las reuniones del CGSR y del CC a través del Grupo de Coordinación para la Protección de Datos en el Ministerio de Justicia.

3. Las funciones de los Delegados de Protección de Datos serán las indicadas en el ya mencionado RGPD, en la LOPDGDD y en la Ley Orgánica 7/2021, de 26 de mayo, y demás disposiciones reguladoras de la materia, y actuarán bajo la coordinación del

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Delegado de Protección de Datos al que incumben las funciones a las que se refiere el artículo 9.5.e) del Real Decreto 453/2020, de 10 de marzo, debiendo contar con los medios personales y materiales necesarios para la realización eficaz de las funciones que tienen encomendadas

Asimismo, los Delegados de Protección de Datos, llevarán a cabo sus funciones de asesoramiento y supervisión respecto de las medidas de seguridad que tengan un objetivo distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales.

4. En virtud del principio de responsabilidad diferenciada, debe existir la necesaria separación de funciones entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS u otras figuras asimiladas, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

Artículo 15. *Análisis y gestión de riesgos de seguridad de la información y de la privacidad.*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.

El proceso de gestión de riesgos comprende 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 ser revisado y actualizado periódicamente.

2. En el tratamiento de los datos personales se llevará previamente a cabo un análisis de riesgos para los derechos y libertades de las personas de conformidad con los artículos 24, 25 y 32 del RGPD y 28 de la LOPDGDD, y en su caso, de acuerdo con los artículos 27, 28 de la Ley Orgánica 7/2021, de 26 de mayo,

3. A los efectos de la seguridad de los datos personales se realizará el análisis de riesgos establecido en el ENS, que complementará el análisis de riesgos de la privacidad.

4. Si el resultado del análisis de riesgos entraña un alto riesgo para los derechos y libertades de las personas físicas, deberá realizarse una evaluación de impacto conforme a lo previsto en el artículo 35 del RGPD, o en su caso, conforme al artículo 35 de la Ley Orgánica 7/2021, de 26 de mayo, sin perjuicio de realizarse en los supuestos previstos en dichos artículos.

5. De conformidad con el artículo 3 del ENS, 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.

6. Los análisis de riesgos indicados en los aparados anteriores se revisarán y aprobarán anualmente, así como cuando se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas, incidentes graves, existencia de vulnerabilidades graves.

Artículo 16. *Auditoría.*

El Ministerio de Justicia llevará a cabo de forma periódica, y al menos cada dos años, una auditoría encaminada a la verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos y sistemas de información.

En todo caso realizará una auditoría específica y extraordinaria cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas.

Las auditorías serán supervisadas por el responsable de seguridad de la información y, en caso de tratamiento de datos personales, por el delegado de protección de datos.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Artículo 17. *Gestión de incidentes de seguridad y violaciones de seguridad de los datos personales.*

1. El Ministerio de Justicia dispondrá de procedimientos de gestión de incidentes de seguridad con los requisitos establecidos en el ENS y su correspondiente instrucción técnica de seguridad.

2. Asimismo, adoptará las medidas necesarias para garantizar la notificación a la autoridad de protección de datos, y las obligaciones de documentación de cualquier violación de la seguridad de los datos personales que pudieran producirse, de conformidad con lo dispuesto en el artículo 33 del RGPD.

Igualmente adoptará las medidas procedentes para la comunicación a los interesados que pudieran haberse visto afectados por la violación de seguridad de los datos de carácter personal, en los casos y conforme a lo dispuesto en el artículo 34 del RGPD.

3. Las obligaciones indicadas en los anteriores apartados se integrarán con sus particularidades específicas en un único procedimiento de gestión de incidentes.

Artículo 18. *Protección de datos de carácter personal.*

El desarrollo normativo de la presente política de garantizarán que por los responsables y encargados del tratamiento de datos se dé cumplimiento a los principios y obligaciones establecidas en el marco normativo de protección de datos con la participación adecuada y en tiempo oportuno, desde el diseño de los tratamientos y sus medios, al delegado de protección de datos, a través de las correspondientes medidas técnicas y organizativas, todo ello a través del marco organizativo de esta PS.

Artículo 19. *Grupos de trabajo.*

El CGSR y el CC, podrán articular la creación de grupos de trabajo para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes.

Artículo 20. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PS prevalecerá la decisión del Comité de Gobierno de Seguridad y Riesgos.

En materia de protección de datos prevalecerán las decisiones del Responsable del Tratamiento de acuerdo con sus competencias y obligaciones.

Artículo 21. *Desarrollo normativo.*

1. El cuerpo normativo de desarrollo de la presente política de seguridad, que podrá dividirse en ámbitos materiales, se desarrollará en tres niveles por ámbito subjetivo de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior.

Con carácter general, y en la medida de lo posible, se procurará la integración de procesos para dar cumplimiento a exigencias de normativas diferentes, sin perjuicio de las particularidades específicas de cada ámbito.

Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Constituido por la PS y las directrices, generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Justicia a los que, conforme al artículo 1, sea de aplicación la presente PS, singularmente la Norma de Seguridad para el uso de los recursos y sistemas.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

b) Segundo nivel normativo: Constituido por las normas de seguridad desarrolladas por cada órgano superior o directivo del Ministerio de Justicia, así como por cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PS. Estas normas de seguridad deberán cumplir los siguientes requisitos:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PS. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo. Sin perjuicio de aquellas normas que sólo puedan ser aplicables a un ámbito o sistema específico, las normas serán desarrolladas a partir de una estructura general y común, donde se adicionarán las especificaciones propias de cada ámbito en caso de existir.

2.º Cumplir estrictamente con lo indicado en el marco normativo aplicable a dicha norma y con el primer nivel normativo enunciado en el presente artículo.

c) Tercer nivel normativo: Constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PS, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel normativo deberá cumplir los siguientes requisitos:

1.º Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PS. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo. Sin perjuicio de aquellos procedimientos que sólo puedan ser aplicables a un ámbito o sistema específico, los procedimientos serán desarrollados a partir de una estructura general y común, donde se adicionarán las especificaciones propias de cada ámbito en caso de existir.

2.º Cumplir estrictamente con lo indicado en el marco normativo aplicable a dicha norma y con el primer y segundo nivel normativos enunciados en el presente artículo.

2. Además de la normativa enunciada en el apartado 1 del presente artículo, la estructura normativa podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a la presente PS 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 PS tendrá la obligación de conocer y cumplir, además de la presente PS, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. El CC 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 PS.

5. Este marco normativo estará a disposición de todos los miembros del Ministerio de Justicia.

Disposición adicional primera. *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.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es

Disposición adicional segunda. *Deber de colaboración en la implantación de la Política de Seguridad.*

Todos los órganos y unidades del Departamento prestarán su colaboración en las actuaciones de implementación de la PS aprobada por esta orden.

Disposición adicional tercera. *Sistemas de información y servicios de tecnologías de la información y de las comunicaciones prestados y gestionados para la Administración de Justicia.*

Los sistemas gestionados por el Ministerio de Justicia para la Administración de Justicia que están sometidos a la Política de Seguridad de la Información de la Administración Judicial Electrónica, aprobada por el Pleno del Comité Técnico de la Administración Judicial Electrónica, de fecha 30 de octubre de 2019, quedan excluidos del ámbito de aplicación de la presente política de seguridad, sin perjuicio de las previsiones contenidas en esta orden ministerial.

Disposición adicional cuarta. *Publicidad.*

Esta orden se publicará en las sedes electrónicas del Ministerio de Justicia en cuyo ámbito sea de aplicación.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden JUS/1293/2017, de 14 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica.

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».

Madrid, 30 de mayo de 2023.–La Ministra de Justicia, María Pilar Llop Cuenca.

cve: BOE-A-2023-13423
Verificable en https://www.boe.es