

I. DISPOSICIONES GENERALES

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

24722 *Orden CNU/1383/2025, de 1 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración digital del Ministerio de Ciencia, Innovación y Universidades.*

Las Tecnologías de la Información y la Comunicación (en adelante, TIC) se han convertido en un mecanismo esencial a la hora de alcanzar los objetivos de cualquier organización pública, suponiendo a su vez, importantes beneficios en cuanto a la eficacia y eficiencia de esta. Por otro lado, la transformación digital del sector público debe incorporar la seguridad de todos los elementos TIC como un elemento más para tener en cuenta: sistemas, comunicaciones, infraestructuras y el propio personal del Ministerio.

Por ello, la seguridad debe considerarse desde una visión integral de los sistemas de información, así como desde un punto de vista global, al cubrir cualquier ámbito que se considere que puede afectar de un modo u otro a la seguridad de los servicios y de la información. Esa necesaria aproximación integral al ámbito de la seguridad de la organización desde el punto de vista TIC proporcionará enfoques preventivos que minimicen la aparición de incidentes (formación, concienciación, medidas técnicas, etc.), como mecanismos de detección y respuesta efectiva a los incidentes a los efectos de garantizar la continuidad de los servicios prestados.

El marco de relación entre la Administración pública y la ciudadanía 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. En su artículo 13 se recoge, entre los derechos de las personas en sus relaciones con las Administraciones públicas, el relativo «a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas».

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3, trata los principios generales relativos a las relaciones de las administraciones a través de medios electrónicos. Así mismo, en su artículo 156 se contempla el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad (en adelante, ENS). Ambas leyes han sido objeto de desarrollo en estas materias en virtud del 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.

Asimismo, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, 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 la ciudadanía 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.

Así, el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo, exige que, en la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Esta política de seguridad se establecerá de acuerdo con los principios básicos recogidos en el capítulo II del citado real decreto, y se desarrollará aplicando los requisitos mínimos referidos en su artículo 12.6, que se refieren a la seguridad como proceso integral, la gestión de la seguridad basada en los riesgos, la prevención, detección, respuesta y conservación, la existencia de líneas de defensa, la vigilancia continua, la reevaluación periódica y la diferenciación de responsabilidades.

Del mismo modo, la Política de Seguridad de la Información debe referenciar y ser coherente con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y

del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; así como en las normas aplicables a la Administración Digital del Departamento que desarrollen o complementen las anteriores y que se encuentren dentro del ámbito de aplicación de la Política de Seguridad de la Información.

En atención a cuanto ha quedado expuesto, el Ministerio de Ciencia, Innovación y Universidades ha situado los sistemas TIC como elementos estratégicos coadyuvantes para el desarrollo y cumplimiento de las competencias que se le atribuyen. Dichos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad de la información tratada, la integridad, la disponibilidad, la autenticidad, o la trazabilidad de los servicios prestados. Los órganos directivos y las unidades administrativas que conforman el Ministerio deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

Así mismo, al disponer de una gran exposición digital a los efectos de proporcionar servicios digitales a ciudadanos y empresas, en diversos ámbitos, así como disponer de procedimientos de control y monitorización en materia de investigación científica y técnica, desarrollo tecnológico, innovación en todos los sectores, entre otros y todo ello en un entorno de amenazas digitales en constante evolución y de distinta naturaleza, la gestión de la seguridad se convierte en una necesidad para el aseguramiento del ejercicio de las funciones encomendadas, siendo imprescindible la implementación de un plan de seguridad que vele por la calidad de los servicios, y la información en sí misma. Un plan que permita gestionar los riesgos relacionados con las TIC y confiera una estructura organizativa y operativa para poder implantar las medidas requeridas.

Finalmente, tanto el personal del Ministerio de Ciencia, Innovación y Universidades como las terceras partes que prestan servicio al mismo, deben ser partícipes del citado plan, ya que su participación es requisito imprescindible tanto para su puesta en marcha, como para lograr la mitigación de los riesgos, estableciéndose un entorno coherente en cuanto a lo que el tratamiento de la seguridad se refiere: la dirección estratégica definiendo las medidas a adoptar para controlar y gestionar los riesgos, el personal técnicos y el usuario final, que se encargan de implantar, configurar, tratar y/o manipular los sistemas de información, así como el personal encargado de medir y supervisar la calidad de las medidas implantadas.

Con la presente orden se pretende, por tanto, aprobar la Política de Seguridad de la Información del Ministerio de Ciencia, Innovación y Universidades, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

Esta 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 de la Información del Ministerio de Ciencia, Innovación y Universidades, y 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 Ciencia, Innovación y Universidades. 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.

Durante su tramitación se ha emitido informe por la Agencia Española de Protección de Datos y por la Agencia Estatal de Administración Digital.

En virtud de lo anterior, con la aprobación previa del Ministro para la Transformación Digital y de la Función Pública, dispongo:

Artículo 1. Objeto y ámbito de aplicación.

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, constituye el objeto de esta orden la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Digital del Ministerio de Ciencia, Innovación y Universidades, así como el establecimiento del marco organizativo global en materia de Seguridad de la Información del Departamento.

2. La PSI será de obligado cumplimiento para todos los órganos del Departamento, así como para los organismos públicos y entidades vinculados o dependientes del mismo que no tengan establecida su propia política de seguridad.

3. La PSI será de obligado cumplimiento para todo el personal en la utilización de medios digitales en el ámbito de actuación del Departamento, la información en soporte papel que gestione en el ámbito de sus competencias, así como para toda persona que acceda tanto a los Sistemas TIC como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con este.

Artículo 2. Marco regulatorio.

1. El marco normativo en que se desarrollan las actividades del Ministerio de Ciencia, Innovación y Universidades, en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, se compone, principalmente, de las siguientes normas:

a) 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.

b) La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

c) La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

d) 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.

e) El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que transpone la Directiva Europea NIS [Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016].

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

g) 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.

h) El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

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

j) 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.

k) El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y las Instrucciones Técnicas de Seguridad para su aplicación dictadas por la persona titular de la Secretaría de Estado de Función Pública, de acuerdo con lo previsto en la disposición adicional segunda de dicho real decreto.

l) Real Decreto 472/2024, de 7 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Ciencia, Innovación y Universidades.

m) 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).

n) 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.

ñ) Las 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.

o) La Directiva (UE) 2022/2555 del Parlamento europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

p) La Ley 9/1968, de 5 de abril, sobre secretos oficiales.

2. Del mismo modo, las actuaciones que desarrolle el Ministerio de Ciencia, Innovación y Universidades en aplicación de esta orden se adecuarán a las normas aplicables a la Administración Electrónica del Departamento que desarrollen o complementen las disposiciones normativas citadas en el apartado anterior vinculadas al ámbito de aplicación de la PSI.

Artículo 3. *Principios de la Política de Seguridad de la Información.*

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 311/2022, de 3 de mayo, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo.

Artículo 4. *Ordenación normativa.*

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

a) Primer nivel. Constituido por la PSI que se aprueba mediante la presente orden.

b) Segundo nivel. Constituido por las normas y directrices generales de seguridad que, respetando lo estipulado por la PSI, determinan el ámbito de uso de los recursos tecnológicos del Departamento y, en su caso, de sus organismos públicos dependientes desde el punto de vista de la seguridad, sin considerar aspectos técnicos relativos a su implementación.

Las normas y directrices generales de seguridad de este segundo nivel normativo serán aprobadas por resolución de la persona titular de la Subsecretaría de Ciencia, Innovación y Universidades, a propuesta del Comité de Seguridad de la Información del Departamento.

c) Tercer nivel: Constituido por los procedimientos, guías, e instrucciones técnicas que sean adoptados cumpliendo con lo expuesto en los niveles normativos anteriores, y que determinan las acciones, tareas o instrucciones de carácter técnico a realizar en el desempeño de un proceso aplicado a ámbitos o sistemas de información particulares.

Su aprobación corresponde a la persona responsable de la Seguridad, previo acuerdo en el Comité de Seguridad de la Información del Departamento.

2. La estructura normativa podrá incorporar asimismo otros instrumentos tales como estándares de seguridad, buenas prácticas, informes técnicos, a criterio de cada

uno de los órganos u organismos comprendidos en el ámbito subjetivo de la presente PSI y siempre dentro del ámbito de sus competencias y responsabilidades.

3. El personal de cada uno de los órganos u organismos comprendidos en el ámbito subjetivo de la presente PSI tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. Este marco normativo estará a disposición de todos los miembros del Departamento y de sus organismos públicos y entidades de derecho público vinculados o dependientes.

Artículo 5. *Estructura organizativa.*

1. La organización de la seguridad debe tener en cuenta la propia organización del Departamento, en consecuencia, las responsabilidades en seguridad de la información deben emerger de todos los ámbitos, garantizándose la actuación coordinada y eficaz, de acuerdo con lo previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre responsabilidades y funciones en el ENS.

2. La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Ciencia, Innovación y Universidades está compuesta por los siguientes agentes:

- a) La persona titular de la Subsecretaría de Ciencia, Innovación y Universidades.
- b) Comité de Seguridad del Departamento.
- c) Responsable de la Seguridad.
- d) Responsable de la Información y Responsable del Servicio.
- e) Responsable del Sistema.
- f) Delegados o Delegadas de Protección de Datos.
- g) Las personas responsables y encargadas del tratamiento de datos personales.
- h) Personas designadas como responsables de la administración de los Sistemas.

Artículo 6. *Competencias de la persona titular de la Subsecretaría de Ciencia, Innovación y Universidades en el ámbito de la Seguridad de la Información.*

1. La persona titular de la Subsecretaría de Ciencia, Innovación y Universidades es, en el ejercicio de sus competencias, de conformidad con lo previsto en los artículos 8.1, apartados d) e i), y 8.2 del Real Decreto 472/2024, de 7 de mayo la responsable de definir, dirigir, planificar, coordinar y supervisar la aplicación de la estrategia sobre tecnologías de la información y las comunicaciones y resto de recursos tecnológicos del Ministerio y de sus diferentes organismos, así como de la implantación de medidas de seguridad informática. A este respecto:

- a) Coordinará todas las actividades relacionadas con la seguridad de los servicios prestados por la Subsecretaría, tanto de carácter horizontal, común o compartido, como de carácter sectorial.
- b) Impulsará la adecuación a la normativa aplicable de seguridad de la información y de protección de datos.
- c) Será responsable de la modificación y actualización de esta PSI, así como de aprobar la normativa de seguridad de segundo nivel propuestas por el Comité de Seguridad de la Información del Departamento.
- d) Será responsable de promover la mejora continua en la gestión de la seguridad de la información en el ámbito del Departamento.

Artículo 7. *El Comité de Seguridad de la Información del Departamento.*

1. Con carácter permanente, se crea el Comité de Seguridad de la Información del Ministerio de Ciencia, Innovación y Universidades (en adelante, Comité) con el objeto de dotar al Departamento de un órgano colegiado de carácter horizontal responsable de

establecer, gestionar, coordinar y supervisar la estrategia en materia de seguridad de la información y el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

2. El Comité estará compuesto por los siguientes miembros:

a) Presidencia: Corresponderá a la persona titular de la División de Tecnologías de la Información (en adelante DVTIC). Tendrá voz y voto de calidad en la toma de decisiones del CSID. Podrá autorizar la asistencia a las reuniones de personas expertas en las materias que se vayan a tratar, ya sean personal interno o externo, que tendrán el carácter de asesores, con voz, pero sin voto.

b) Vocales:

1.º La persona designada como Responsable de los Sistemas.

2.º Las personas designadas como Responsables de la Información, y como Responsables de los Servicios en el ámbito del Departamento.

3.º La persona designada como Delegado o Delegada de Protección de Datos del Ministerio de Ciencia, Innovación y Universidades, y como Delegados y Delegadas de Protección de Datos de los organismos públicos adscritos al Ministerio. Actuarán, con voz, pero sin voto, para garantizar su independencia en atención a la naturaleza de sus funciones de apoyo y asistencia.

c) Secretaría: Corresponderá a la persona designada como Responsable de la Seguridad del Departamento, que tendrá voz y voto y que ejecutará las decisiones del comité director, convocará sus reuniones y preparará los temas a tratar.

3. Podrá formar parte como vocal una persona responsable de los organismos y entidades dependientes del Ministerio, con voz y voto, en caso de que fuera necesario y así lo determine la persona titular de la Presidencia.

4. La persona titular de la Presidencia podrá convocar, debido a los asuntos a tratar, a representantes de cualquier órgano y unidad que accedan a sistemas de información del Departamento, así como a personal experto en calidad de asesores, que actuarán con voz, pero sin voto.

5. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona a la que corresponda la Presidencia será sustituida por el miembro del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden.

6. El Comité se reunirá con carácter ordinario, una vez al año o con carácter extraordinario cuando la Presidencia lo considere necesario si:

a) Surgieran incidencias de seguridad graves.

b) Fuera necesario establecer nuevas directrices de seguridad.

c) Existiera una solicitud motivada de la persona designada Responsable de la Seguridad.

7. Son funciones del Comité:

a) Elaborar estudios, análisis y propuestas de modificación y actualización de la Política de Seguridad, de la estrategia de evolución del Departamento en el ámbito de la seguridad y de la normativa de seguridad de la información de segundo nivel, incluyendo el protocolo de actuación y de gestión de incidentes de seguridad que existe hoy en día en el Ministerio y a disposición del Comité para su actualización si así lo considera oportuno.

b) Velar por la coherencia y armonización de la normativa y actuaciones en materia de seguridad de la información entre los distintos servicios ofrecidos por los órganos del Departamento, ya sean los de carácter común, horizontal o sectorial.

c) Estudiar y proponer actividades de concienciación y formación en materia de seguridad, velar e impulsar el cumplimiento del cuerpo normativo a que se refiere el

artículo 4, e impulsar y promover la formación y concienciación en materia de seguridad de la información.

d) Realizar cualquier otra actividad de asesoría, formulación de recomendaciones, o propuesta de iniciativas, en materia de seguridad.

e) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento, así como la evaluación y seguimiento de las decisiones tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.

f) Informar periódicamente a la persona titular de la Subsecretaría de Ciencia, Innovación y Universidades sobre el estado de la seguridad en el ámbito de esta Política de Seguridad. Para ello, podrá utilizar informes de incidentes de seguridad, resultados de auditorías y análisis de riesgos realizados y, en general, cualquier información de seguridad relevante que pueda recabar en el desarrollo de sus funciones.

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

8. En el establecimiento de los acuerdos y toma de decisiones serán tenidos en cuenta todos los miembros del Comité.

9. El Comité 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.

Artículo 8. *Responsable de la Seguridad.*

1. La persona designada Responsable de la Seguridad (de los sistemas de información), será nombrada por la persona titular de la DVTIC, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENSF, y le corresponde determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportar sobre estas cuestiones.

2. El ámbito de actuación de la persona designada Responsable de la Seguridad se extiende a todos los servicios de tecnologías de la información y las comunicaciones prestados y/o gestionados por el Departamento, debiendo velar por la coherencia y armonización de las normas, procedimientos y actuaciones en los diferentes ámbitos.

3. Le corresponde el desempeño de las siguientes funciones:

a) Elaborar la normativa de seguridad de segundo nivel, definida en el artículo 4, así como aprobar los procedimientos, guías, e instrucciones técnicas vinculadas al tercer nivel normativo, previo acuerdo en el Comité.

b) Mantener la documentación de seguridad actualizada y organizada, así como gestionar los mecanismos de acceso a esta.

c) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios y proponer las decisiones respecto a las medidas de que considere imprescindibles para preservar la seguridad, integridad y disponibilidad de los servicios prestados y la información manejada por el Departamento.

d) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, y coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

e) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

4. La persona designada Responsable de la Seguridad no podrá ser designada como Responsable de la Información, ni de los Servicios. Adicionalmente, deberá ser

distinta del Responsable de los Sistemas y no podrá existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que la función de Responsable de la Seguridad y la función de Responsable de los Sistemas recaiga en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del Real Decreto 311/2022, de 3 de mayo.

Artículo 9. *Responsable de los Sistemas.*

1. La persona designada Responsable de los Sistemas (de información), será nombrada por la persona titular de la DVTIC, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, y es la persona encargada de la explotación de los sistemas de información de su ámbito específico de competencias, así como de desarrollar la forma concreta de implementar la seguridad en los sistemas y de la supervisión de la operación diaria de los mismos.

Este ámbito vendrá determinado por los sistemas de información, los tratamientos de datos personales y servicios de tecnologías de la información y de las comunicaciones que sean prestados y/o gestionados directamente por la DVTIC.

2. Las funciones que corresponden a la persona designada Responsable de los Sistemas son:

- a) Definir la tipología y sistema de gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en este.
- b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco tecnológico y de seguridad del Departamento.
- c) Suspender el tratamiento de una determinada información o la prestación de un determinado servicio electrónico si es informado o detecta deficiencias graves de seguridad, previo acuerdo con la persona designada Responsable de la Seguridad y con el conocimiento previo de la persona designada Responsable de dicha Información o de dicho Servicio.
- d) Cualquier otra función en el ámbito de la seguridad de los sistemas de información que le sea encomendada a través de las diferentes normativas y procedimientos de seguridad.

3. La persona designada Responsable de los Sistemas podrá designar motivadamente, siendo responsable de su actuación, a las personas designadas como Administradores o Administradoras de los Sistemas que considere necesarias para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

Artículo 10. *Responsables de la Información.*

1. Las personas designadas Responsables de la Información, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, tienen la competencia, dentro de su ámbito de actuación y competencias, de aprobar los requisitos en materia de seguridad de la información que manejan y, por tanto, de su protección. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos (Ley Orgánica 3/2018, de 5 de diciembre).

2. Serán funciones de las personas designadas Responsables de la Información, dentro de sus ámbitos de actuación, las siguientes:

- a) Determinar los niveles de seguridad de la información tratada valorando los impactos de los incidentes que afecten a la seguridad de la información.

b) Son las encargadas, junto a las personas designadas Responsables de los Servicios y contando con la participación de la persona designada Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

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

d) Son las responsables últimas de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información tratada dentro de su ámbito de actuación y competencias.

e) Tienen la responsabilidad última del uso y acceso que se haga de la información de la que son responsables y, por tanto, de su mantenimiento y protección.

f) Cualquier otra función en el ámbito de la seguridad de la información que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. La designación de las personas Responsables de la Información, con rango mínimo de Subdirector General, corresponderá a la persona titular de cada órgano superior o directivo, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, de acuerdo con su propia organización interna.

Artículo 11. *Responsables de los Servicios.*

1. Las personas designadas Responsables de los Servicios, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, tienen la competencia, dentro de su ámbito de actuación y competencias, de aprobar los requisitos en materia de seguridad de los servicios que prestan y, por tanto, de determinar los niveles de seguridad de dichos servicios.

2. Serán funciones de las personas designadas Responsables de los Servicios, dentro de sus ámbitos de actuación, las siguientes:

a) Determinar los niveles de seguridad de los servicios prestados valorando los impactos de los incidentes que afecten a la seguridad del servicio.

b) Son las encargadas, junto a las personas designadas Responsables de la Información y contando con la participación de la persona designada Responsable de la Seguridad, de realizar los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

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

d) Cualquier otra función en el ámbito de la seguridad de los servicios que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. La designación de las personas Responsables de los Servicios, con rango mínimo de Subdirector General, corresponderá a la persona titular de cada órgano superior o directivo del Departamento, y de cada organismo público dependiente del Ministerio a los que sea de aplicación esta PSI, de acuerdo con su propia organización interna, con rango mínimo de Subdirector General.

Artículo 12. *Delegado o Delegada de Protección de Datos.*

1. La persona designada Delegado o Delegada de Protección de Datos (en adelante DPD) ejerce las funciones detalladas en la sección 4 del capítulo IV del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y en el capítulo III del título V de la Ley Orgánica 3/2018, de 5 de diciembre. Tendrá en todo caso acceso al registro de las actividades de tratamiento de datos personales al que se refiere el artículo 30 del Reglamento (UE) 2016/679.

2. El DPD desempeñará las funciones detalladas en la sección 4 del capítulo IV del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril

de 2016, y en el capítulo III del título V de la Ley Orgánica 3/2018, de 5 de diciembre, y demás disposiciones reguladoras de la materia.

La actuación del DPD se regirá por el principio de independencia, por lo que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrá estar asistido por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.

3. A fin de garantizar su independencia y evitar cualquier tipo de conflicto de intereses en el ejercicio de sus funciones, no podrá coincidir en la misma persona la designación del DPD y como Responsable de la Seguridad. Así mismo, entre las personas designadas para los citados cargos, no existirá ningún tipo de dependencia funcional u orgánica.

Artículo 13. Responsable y Encargado o Encargada del tratamiento de datos personales.

1. La persona designada Responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otra entidad que, solo o junto con otros, determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.

2. La identidad de la persona designada Responsable del tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del Reglamento General de Protección de Datos.

3. La persona designada como Encargado o Encargada 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.

Artículo 14. Protección de datos de carácter personal.

1. En el ámbito del Ministerio de Ciencia, Innovación y Universidades, la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del Departamento, que se rige por los principios recogidos en el artículo 5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento, aplicándose para ello las medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos, tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre. Dicho análisis de riesgos se realizará teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

El cumplimiento de este principio corresponde a la persona designada Responsable del tratamiento que, adicionalmente, debe ser capaz de demostrarlo y aplicarlo de forma temprana en la fase de diseño del tratamiento y garantizando que su aplicación sea efectiva por defecto.

3. La garantía del cumplimiento de lo previsto en el apartado anterior, se articulará a través del marco organizativo establecido en la presente Política de Seguridad y se llevará a cabo de conformidad con la normativa aplicable en materia de protección referida en el artículo 3 de esta orden y en el Real Decreto 311/2022, de 3 de mayo, prevaleciendo las medidas derivadas de la aplicación de la normativa de protección de

datos cuando, tras un análisis de riesgos, se estime que las mismas son superiores a las previstas en el ENS.

4. La observación del principio de seguridad del tratamiento de los datos personales cobrará especial relevancia cuando sea probable que un determinado tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, en cuyo caso la persona designada Responsable del tratamiento recabará el asesoramiento del DPD al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

5. Las auditorías de seguridad previstas en el Esquema Nacional de Seguridad incorporarán la revisión de las medidas técnicas y organizativas de seguridad de los datos personales a las que se refiere este artículo.

Artículo 15. *Administradores o Administradoras de los Sistemas.*

1. Las personas designadas Administradores o Administradoras de los Sistemas, que serán nombradas por la persona designada Responsable de los Sistemas, de acuerdo con lo previsto en el artículo 13 del Real Decreto 311/2022, de 3 de mayo, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, son las personas responsables de la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información y de la aplicación de los Procedimientos Operativos de Seguridad.

2. Son funciones de las personas designadas Administradores o Administradoras de los Sistemas:

a) Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

b) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

c) Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

d) Cualquier otra función en el ámbito de la administración de seguridad que le sea encomendada a través de la normativa de seguridad de segundo nivel al respecto.

3. Las personas designadas Administradores o Administradoras de los Sistemas tendrán dependencia funcional directa de la persona designada como Responsable de los Sistemas.

Artículo 16. *Resolución de conflictos.*

En caso de conflicto entre las personas designadas como responsables, de conformidad con lo previsto en la presente orden, corresponderá al superior jerárquico su solución, si pertenecen al mismo órgano superior del Departamento. En otro caso, la resolución corresponderá a la persona titular de la Subsecretaría de Ciencia, Innovación y Universidades.

Disposición adicional primera. *Política de seguridad de la información de los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Ciencia, Innovación y Universidades.*

1. De acuerdo con lo previsto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, y el artículo 1.2 de esta orden, los organismos y entidades vinculados, dependientes o adscritos al Ministerio de Ciencia, Innovación y Universidades podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento aprobada por esta orden.

2. En caso de discrepancia, prevalecerá la política de seguridad de la información definida en esta orden ministerial.

3. En todo caso, los organismos públicos vinculados o dependientes del Departamento deberán informar de forma inmediata a la División de Tecnologías de la Innovación sobre cualquier incidencia o riesgo que pueda poner en peligro la seguridad de los sistemas informáticos del Departamento.

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

La aplicación de esta orden no conllevará incremento del gasto público, ni supondrá incremento de dotaciones, ni de retribuciones u otros gastos de personal.

Disposición adicional tercera. *Actualización permanente y revisiones periódicas de la PSI.*

1. Esta orden deberá mantenerse actualizada para adecuarla al progreso de los servicios de la Administración Digital, a la evolución tecnológica y al desarrollo de la sociedad de la información.

2. Las propuestas de las sucesivas revisiones de la PSI corresponden al Comité.

Disposición adicional cuarta. *Deber de colaboración en la implantación de la PSI.*

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

Disposición adicional quinta. *Aplicación de la PSI a la Agencia Estatal de Investigación y a la Agencia Estatal «Agencia Espacial Española».*

Esta PSI será de aplicación a la Agencia Estatal de Investigación y a la Agencia Estatal «Agencia Espacial Española», hasta el momento en que dichas agencias dejen de compartir completamente sus sistemas y servicios informáticos con el Departamento.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta orden y, en particular, la Orden UNI/1231/2021, de 5 de noviembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica y de protección de datos y se crea la Comisión Ministerial de Administración Digital del Ministerio de Universidades, en lo que contradiga a la presente orden.

Disposición final primera. *Instrucciones de ejecución.*

La persona titular de la Subsecretaría de Ciencia, Innovación y Universidades podrá dictar las instrucciones necesarias para la ejecución y aplicación de esta orden, de conformidad con lo previsto en el artículo 6 de la Ley 40/2015, de 1 de octubre.

Disposición final segunda. *Publicidad de la PSI.*

Esta orden se publicará en el «Boletín Oficial del Estado», así como en el portal institucional del Ministerio de Ciencia, Innovación y Universidades.

Disposición final tercera. *Entrada en vigor.*

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

Madrid, 1 de diciembre de 2025.—La Ministra de Ciencia, Innovación y Universidades, Diana Morant Ripoll.