

0060/2025**I**

El proyecto de Orden tiene por objeto la aprobación de la Política de Seguridad de la Información (PSI) en el ámbito de la Administración Digital del Ministerio de Ciencia, Innovación y Universidades, de acuerdo con lo previsto en su artículo 1. La norma establece el marco organizativo global en materia de seguridad de la información del Departamento, así como las directrices generales que rigen la gestión y protección de la información tratada y de los servicios electrónicos prestados.

La Orden se dicta en cumplimiento de lo dispuesto en el artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), que dispone que cada ministerio de la Administración General del Estado contará con su propia política de seguridad, aprobada por la persona titular del Departamento. Asimismo, se ajusta a los principios básicos y requisitos mínimos establecidos en los artículos 5 y 12.6 del citado Real Decreto.

La PSI objeto de análisis se enmarca, además, dentro de las competencias atribuidas al Departamento por el Real Decreto 472/2024, de 7 de mayo, por el que se desarrolla su estructura orgánica básica. Este Real Decreto atribuye al Ministerio de Ciencia, Innovación y Universidades la dirección, coordinación y ejecución de las políticas gubernamentales en materia de investigación científica y técnica, desarrollo tecnológico e innovación en todos los sectores, así como la representación de España en los organismos e instituciones internacionales en la materia.

La Orden proyectada articula una estructura organizativa coherente con lo previsto en el ENS y normativa complementaria sobre roles y funciones. De tal modo, regula la composición y funciones del Comité de Seguridad de la Información, la figura del Responsable de Seguridad, los Responsables de la Información, del Servicio y de los Sistemas, así como las funciones del Delegado de Protección de Datos —DPD— y del Responsable del tratamiento.

Esta estructura garantiza la necesaria diferenciación de responsabilidades, la independencia funcional del DPD, y la existencia de mecanismos de supervisión y coordinación, de acuerdo con lo dispuesto en los artículos 11 y 13 del Real Decreto 311/2022, de 3 de mayo.

En este sentido, debe recordarse que el citado Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS, en su artículo 12.3, prevé que “En

*la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento”, disponiéndose en el apartado 6 del propio artículo 12, que la política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los requisitos mínimos que en dicho Esquema Nacional se contemplan. **Por otra parte, esta PSI se dirige a garantizar el debido cumplimiento de lo dispuesto en la normativa de protección de datos.***

El artículo 2 de la Orden establece el marco normativo aplicable a las actuaciones del Ministerio en materia de seguridad de la información, incluyendo un conjunto de normas nacionales y europeas que configuran el entorno jurídico en el que se desenvuelve la PSI. En lo que aquí interesa, se remite expresamente al Reglamento (UE) 2016/679, de 27 de abril de 2016, y a la Ley Orgánica 3/2018, de 5 de diciembre, en materia de protección de datos personales.

La Orden articula su contenido conforme a los principios rectores recogidos en su artículo 4, entre los cuales cabe destacar los de seguridad integral, gestión de riesgos, proporcionalidad, mejora continua y seguridad desde el diseño y por defecto, plenamente alineados con el RGPD y el ENS:

“Artículo 4. Principios rectores de la Política de Seguridad.

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, y, por tanto, la presente política de seguridad se establece de acuerdo los siguientes principios:

(...)

b) Responsabilidad diferenciada. En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. **En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.** (La negrita es nuestra)

(...)

d) Gestión de Riesgos. De acuerdo con lo establecido en los **artículos 24, 25 y 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 7 del Real Decreto 311/2022, de 3 de mayo, el análisis y gestión de riesgos será parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.**

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de 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. **Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.** (La negrita es nuestra)

(...)

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, **debiendo tener en cuenta la protección de datos personales en los supuestos en que aplique.** (La negrita es nuestra)

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

a) **Protección de datos personales. Se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. 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 Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser proporcionales en función del análisis de riesgos, así como de una evaluación de impacto** relativa a la protección de datos, poniendo máximo énfasis cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas. (La negrita es nuestra)

(...)"

Pues bien, según se observa, estos principios configuran el marco general en el que se integran las medidas de seguridad y las obligaciones en materia de protección de datos de carácter personal, garantizando la coherencia entre la seguridad de la información y la protección de los derechos fundamentales de las personas físicas. Así, de acuerdo con la regulación del artículo 4 del proyecto de Orden, el redactor de la norma ha considerado en el marco de la confección y aplicación de su PSI —de manera plena, precisa y conforme con la normativa aplicable—, el conjunto de las cuestiones más importantes atinentes a la protección de los datos de carácter personal.

II

El **artículo 15** de la Orden que se informa constituye el núcleo de la regulación en materia de **protección de datos personales** dentro de la PSI ministerial. Dicho precepto desarrolla, de forma coherente con el marco europeo y nacional aplicable, los principios, garantías y medidas técnicas y organizativas que deben regir el tratamiento de datos personales en el ámbito del Ministerio de Ciencia, Innovación y Universidades. Según dispone:

“Artículo 15. *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 **siguientes principios**:

- a) Licitud, lealtad y transparencia.
 - b) Limitación de la finalidad.
 - c) Minimización de datos.
 - d) Exactitud.
 - e) Limitación del plazo de conservación.
 - f) Integridad y confidencialidad.
 - g) Responsabilidad proactiva.
- (La negrita es nuestra)

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. (La negrita es nuestra)

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.** (La negrita es nuestra)

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.** (La negrita es nuestra)

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.** (La negrita es nuestra)

A la vista de la transcrita regulación, se aprecia que se reconocen amplia, coherente y ordenadamente el conjunto de principios del tratamiento de los datos personales. Esto es, el apartado 1 del artículo 15 recoge dichos **principios generales** aplicables al tratamiento de datos personales: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y responsabilidad proactiva, de manera expresa e indubitada, concediéndoles con su reconocimiento expreso la importancia que merecen.

Se trata de una transposición fiel del contenido del artículo 5 del RGPD y del artículo 4 de la LOPDGDD, que garantiza la aplicación efectiva de dichos principios a todas las unidades del Departamento y organismos vinculados o dependientes.

En cuanto a la **seguridad del tratamiento y análisis de riesgos**, el apartado 2 del artículo que se analiza establece que la seguridad de los datos personales constituye uno de los principios rectores del tratamiento, imponiendo la adopción de medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado al riesgo. Esta previsión se ajusta plenamente a lo dispuesto en los artículos 24 y 32 del RGPD y en el artículo 28 de la LOPDGDD, al exigir la realización de un análisis de riesgos previo y la evaluación de impacto en los casos en que sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

El cumplimiento de este principio corresponde al Responsable del tratamiento, quien debe ser capaz de demostrar la conformidad del tratamiento con la normativa aplicable, aplicando el principio de “seguridad desde el diseño y por defecto” (en relación con lo previsto en el artículo 4 del proyecto de Orden).

En cuanto a la coordinación entre la normativa de protección de datos y el ENS, el apartado 3 del artículo 15 introduce una previsión relevante al establecer que, en caso de divergencia entre las medidas derivadas del ENS y las resultantes del análisis de riesgos conforme a la normativa de protección de datos, prevalecerán las más estrictas derivadas del RGPD y la LOPDGDD.

De tal modo, en relación con el tratamiento de datos de carácter personal, el artículo 15 de la Orden prevé expresamente que las medidas de seguridad apropiadas en cada caso, derivadas del análisis de riesgos, así como la realización de una evaluación de impacto relativa a la protección de datos, podrán concretarse en determinadas **medidas agravadas respecto a las que hayan de aplicarse conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Dichas medidas serán las que correspondan en atención a lo dispuesto en el RGPD y en la LOPDGDD.**

Esta cláusula de prevalencia constituye una **garantía de protección reforzada** en materia de protección de datos, y una adecuada articulación entre las exigencias del Esquema Nacional de Seguridad y las normas específicas sobre datos personales.

La previsión de adopción de **medidas agravadas** a consecuencia del análisis de riesgos responde a lo establecido en el art. 3.3 del Real Decreto 311/2022, de 3 de mayo, según se ha venido señalando en los informes emitidos por esta Agencia, por todos el **Informe 170/2018**, de 12 de noviembre de 2018, que recordó la diferenciación entre la figura del Delegado de Protección de Datos y el Responsable de Seguridad, que, por su interés al caso, reproducimos en lo procedente:

“Con carácter previo a analizar la concreta cuestión planteada en la consulta, este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan.

En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados “Tecnologías de la Información y las Comunicaciones -TIC-”), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, cuyo Preámbulo señala que “la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios” añadiendo que “en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles”.

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro

Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 “no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos”.

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

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

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

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

contencioso-administrativa.

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

Y en este mismo sentido se pronuncia 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que tiene por objeto “proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales” (artículo 1.2.), destacando en su Considerando 1 que “la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental” y en su Considerando 10 que “para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo”.

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento” y “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el

desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para “asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento” (artículo 57.1.c) RGPD)”.

En síntesis, tal y como ha venido informando esta Agencia, las medidas a implantar como consecuencia del análisis de riesgos previsto en el artículo 32 del RGPD, **en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre éstas últimas**, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

En consecuencia, esta Agencia considera **favorablemente las previsiones del artículo 15 de la Orden** sometida a informe, en la que se dispone que, cuando el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el Anexo del Esquema Nacional de Seguridad —actualmente reguladas en el Real Decreto 311/2022, de 3 de mayo—, las medidas derivadas de dicho análisis serán las que deban implementarse en aras de la protección de datos de carácter personal (teniéndose así en cuenta lo dispuesto en el artículo 32 del RGPD relativo a la “Seguridad del Tratamiento”).

III

El **artículo 13 de la Orden** regula detalladamente la figura del **Delegado** o Delegada de Protección de Datos (DPD), estableciendo su independencia funcional y la prohibición de que coincida con el Responsable de Seguridad, a fin de evitar conflictos de intereses, conforme a lo exigido por el artículo 38 del Reglamento (UE) 2016/679 y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre.

Esta regulación resulta adecuada y coherente con los criterios interpretativos de la Agencia Española de Protección de Datos, según se viene señalando en los informes emitidos con relación a las políticas de seguridad de la información aprobadas por distintos departamentos ministeriales.

El citado precepto configura con la necesaria amplitud la figura y funciones del Delegado de Protección de Datos del Ministerio, en términos análogos a los previstos en la Sección 4 del Capítulo IV del Reglamento General de Protección de Datos y en el Capítulo III del Título V de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

El Delegado ejercerá las funciones de **asesoramiento y supervisión** en el ámbito de la Orden, prestando asistencia a los responsables del tratamiento

en la identificación de riesgos, la adopción de medidas de protección y su efectiva puesta en práctica.

De acuerdo con lo dispuesto en el artículo 37 del RGPD y en el artículo 34 de la Ley Orgánica 3/2018, la designación del DPD deberá efectuarse conforme a la legislación aplicable en materia de protección de datos, atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y de la práctica en materia de protección de datos, así como a su capacidad para desempeñar las funciones que tiene encomendadas.

En este sentido, el Delegado o Delegada de Protección de Datos deberán informar y asesorar a los responsables del tratamiento sobre las obligaciones que les incumben en virtud del RGPD, supervisar el cumplimiento de la normativa de protección de datos personales en el Departamento, y ofrecer asesoramiento especializado y actuar como interlocutor entre los responsables del tratamiento y las autoridades de control en materia de protección de datos.

Asimismo, el apartado 4 del artículo 15 prevé la intervención del DPD en los supuestos en que un tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, conforme a lo dispuesto en el artículo 35 del RGPD, garantizando así la supervisión y el asesoramiento en la realización de la correspondiente evaluación de impacto.

En consecuencia, **las previsiones contenidas en los artículos 13 y 15.4 de la Orden resultan plenamente conformes con la normativa en materia de protección de datos personales**, reflejando una regulación coherente con el marco jurídico europeo y con los criterios interpretativos de la autoridad de control.

Según se viene exponiendo, una función importante del Delegado de Protección de Datos es la de prestar al Responsable del tratamiento la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas de seguridad, así como supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el DPD asesora al Responsable y controla el cumplimiento de las obligaciones establecidas por la normativa de protección de datos de carácter personal.

En este sentido, el documento de Directrices sobre los delegados de protección de datos, adoptado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, el 13 de diciembre de 2016 y revisado el 5 de abril de 2017 (documento WP243), aclara que *“El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar «medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (artículo 24, apartado 1).*

El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del Responsable del tratamiento, no del DPD”.

En lo que al articulado del texto que se informa atañe, las funciones atribuidas al Delegado encajan claramente con su función de asesoramiento y consulta, así como en el ámbito de sus relaciones con el resto de los órganos del responsable. Asimismo, el DPD deberá relacionarse tanto con los sujetos afectados por los tratamientos, como con las Administraciones públicas competentes, y, especialmente, con las autoridades de control en materia de protección de datos.

Además, según se regula en el artículo 8.2. 3º de la Orden, en lo relativo a su participación en las reuniones del “Comité de Seguridad de la Información del Departamento”, su papel y funciones se desarrollarán únicamente en calidad de *invitado*. Asimismo, idéntico papel y funciones (“de invitado”) deberán considerarse en cuanto a su participación en las reuniones del resto de Comités y/o Comisiones establecidas en la Orden.

De tal modo, según dispone el citado precepto:

“Artículo 8. El Comité de Seguridad de la Información del Departamento.

(...)

2)

(...)

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.**” (La negrita es nuestra)

En este sentido, la función de asesoramiento del Delegado de Protección de Datos, así como la naturaleza de su figura —caracterizada por la autonomía e independencia de su actuación—, apuntan a la necesidad de que su participación en los citados órganos tenga lugar únicamente en atención a la naturaleza de sus funciones de apoyo y asistencia. La garantía del eficaz desempeño de sus funciones exige que su participación en dichos órganos colegiados se produzca únicamente *con voz, pero sin voto*, por cuanto el propio Delegado deberá velar por el control y cumplimiento por parte del Responsable del tratamiento de las obligaciones establecidas por la normativa de protección de datos.

Así se señaló ya, entre otros, en los Informes 85/2022, referido a la PSI del Ministerio de Asuntos Económicos y Transformación Digital, en el 103/2022, relativo a la PSI del Ministerio de Trabajo y Economía Social, en el 36/2024 respecto a la PSI del Ministerio de Inclusión, Seguridad Social y Migraciones, y en el 20/2025 en relación con la PSI del Ministerio de Educación, Formación Profesional y Deportes.

Por todo ello, se **informa favorablemente** el contenido del **artículo 13** del proyecto de Orden, en tanto regula con la debida amplitud, precisión y adecuación las cuestiones relativas a la designación, funciones e independencia del Delegado de Protección de Datos, garantizando la correcta aplicación de los principios y obligaciones establecidos en el RGPD y la LOPDGDD.

IV

En cuanto a la gestión de la seguridad en el Ministerio, la Orden que se informa desarrolla en sus artículos 6 a 12 la estructura organizativa en materia de seguridad, definiendo los órganos y figuras responsables de su implantación y seguimiento. Destacan la Subsecretaría del Departamento, el Comité de Seguridad de la Información y las personas designadas como Responsables de Seguridad, de los Sistemas, de la Información y de los Servicios, además de los Administradores o Administradoras de los Sistemas.

La Subsecretaría ejerce la dirección y supervisión de la estrategia de seguridad, impulsando la mejora continua y la adecuación normativa. El Comité de Seguridad, presidido por la División de Tecnologías de la Información, coordina y evalúa la estrategia de seguridad del Ministerio, vela por el cumplimiento del Esquema Nacional de Seguridad y promueve la formación, la gestión de incidentes y la coherencia entre las actuaciones de los distintos órganos.

El Responsable de Seguridad garantiza la correcta aplicación de las medidas de protección y coordina la respuesta ante incidentes, actuando con independencia del Responsable de los Sistemas. Este último gestiona la operación técnica de los sistemas, asegurando su integridad y disponibilidad, y puede delegar tareas en los Administradores o Administradoras de los Sistemas, encargados de implementar y mantener las medidas de seguridad operativas.

Los Responsables de la Información y de los Servicios determinan los requisitos de seguridad aplicables a los datos y servicios de su ámbito, participan en los análisis de riesgos y asumen los riesgos residuales. Cuando se trate de información con datos personales, deberán aplicar las garantías previstas en el RGPD y en la LOPDGDD.

Por su parte, el apartado 5 del artículo 15 dispone que las auditorías de seguridad previstas en el Esquema Nacional de Seguridad incluirán la revisión de las medidas técnicas y organizativas aplicadas al tratamiento de los datos personales. Esta previsión refuerza la necesaria interrelación entre las auditorías ENS y las auditorías de protección de datos, garantizando la coherencia y complementariedad de los mecanismos de control.

Todo este entramado organizativo se sustenta en los principios rectores establecidos en el artículo 4 de la Orden, que configuran la política de seguridad de la información del Ministerio de Ciencia, Innovación y Universidades. Entre ellos destacan el compromiso institucional y estratégico de toda la estructura organizativa, la seguridad integral y continua, la proporcionalidad de las medidas en función de los riesgos, la gestión activa y permanente de dichos riesgos, la diferenciación de responsabilidades y la incorporación de la seguridad desde el diseño y por defecto. Estos principios, en consonancia con lo dispuesto en el Real Decreto 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad, garantizan una gestión coherente, segura y sostenible de la información y de los servicios digitales del Departamento.

Asimismo, la Orden desarrolla de forma detallada estos principios de seguridad de la información, sobre los cuales se articula la implantación de las medidas técnicas y organizativas necesarias para la protección de los activos del Ministerio. Dichos principios abarcan el compromiso estratégico de la dirección, el enfoque integral basado en riesgos, la prevención, detección y respuesta ante incidentes, la existencia de múltiples líneas de defensa, la vigilancia continua, la mejora permanente de la seguridad, y la incorporación de la protección de datos personales en todo el ciclo de vida de los sistemas, conforme a lo previsto tanto en el Real Decreto 311/2022, de 3 de mayo, como en el RGPD.

V

Por lo demás, según se advierte, el texto que se informa considera la evolución de las políticas de seguridad de la información desde un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos (responsabilidad proactiva, art. 5.2 RGPD), quedando dicho enfoque claramente plasmado en el texto que se informa, con estricta observancia de los artículos 24 y 32.1 del RGPD, y en consonancia con las previsiones de su Considerando 75.

La determinación de las diferentes funciones asignadas en los artículos 6 a 12 —referidos a la estructura, organización y medidas de seguridad— y en el artículo 13 de la Orden —en relación con el Delegado de Protección de Datos— respetan el esencial conocimiento que este debe poseer de la política de seguridad de la información, participando dicho DPD con su asesoramiento en su implantación en virtud de las funciones que le otorga expresamente el RGPD.

A su vez, en cuanto a la *compatibilidad funcional del Delegado de protección de datos del RGPD y el Responsable de Seguridad* del Esquema Nacional de Seguridad, tal y como se indicó en nuestro **Informe 170/2018**, **la orden deslinda claramente los ámbitos de actuación de ambas figuras.**

Por otro lado, resulta esencial identificar la figura del **Responsable del tratamiento** que —según se señala claramente en el artículo 14 del proyecto de Orden— será la persona, organismo o unidad responsable del tratamiento y, en su caso, al **Encargado del Tratamiento**, que será 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. Las personas designadas 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.”

En conclusión, el proyecto de Orden analizado cumple con las exigencias en materia de protección de datos personales, al prever expresamente el pleno sometimiento a su normativa, la realización del correspondiente análisis de riesgos y, en su caso, de la evaluación de impacto, en aquellos sistemas que traten datos personales, conforme al RGPD y a la LOPDGDD, garantizando, además, el respeto al conjunto de principios relativos al tratamiento del artículo 5 RGPD.

Asimismo, en el artículo 15 del proyecto de Orden se contiene de manera específica una amplia y completa regulación del tratamiento de los datos de carácter personal.

A su vez, el proyecto de Orden desarrolla detalladamente la metodología de gestión de riesgos y la asignación de responsabilidades, asegurando la prevalencia de la normativa de protección de datos en todo el proceso. Así, cuando dichas medidas resulten más estrictas que las del Esquema Nacional de Seguridad, deberán prevalecer sobre estas últimas para garantizar el cumplimiento adecuado del RGPD.

Por último, el proyecto contempla con la debida atención que el Delegado de Protección de Datos deberá desempeñar labores de asesoramiento y supervisión en el ámbito de aplicación de la Orden, prestando apoyo a los responsables del tratamiento en la identificación de riesgos, la adopción de medidas de protección y la verificación de su correcta implantación y ejecución.

El texto proyectado establece un marco adecuado de garantías, tanto en lo relativo a los principios de tratamiento como en la gestión de riesgos, la prevalencia de las medidas más exigentes de protección de datos, la evaluación de impacto y la independencia del Delegado de Protección de Datos.

A la vista del análisis realizado, **se considera que el contenido del proyecto de Orden se ajusta plenamente a la normativa europea y nacional aplicable en la materia, en particular al RGPD y a la LOPDGDD. Por todo ello, se informa favorablemente el proyecto de Orden por la que se aprueba la Política de Seguridad de la Información del Ministerio de Ciencia, Innovación y Universidades, así como su coherencia general la normativa aplicable en materia de protección de datos personales.**