

**0040/2024****I**

Tal y como dispone el artículo 1.1 del texto sometido a informe constituye su objeto la aprobación de la Política de Seguridad de la Información (en adelante **PSI**) en el ámbito de la Administración Digital del Ministerio de Hacienda, así como su marco organizativo y tecnológico, que será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación.

El texto de la orden responde, de una parte, (i) a la necesidad de adecuar la referida política a las exigencias derivadas de la entrada en vigor del nuevo Esquema Nacional de Seguridad (**ENS**), aprobado por Real Decreto 311/2022, de 3 de mayo, cuyo 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, y, de otra parte, (ii) a garantizar el debido cumplimiento de lo dispuesto en la normativa de protección de datos.

De este modo, el artículo 4 del proyecto desarrolla los principios de seguridad de la información, así como los objetivos que garantizan su cumplimiento.

Igualmente se desarrolla la estructura organizativa del Departamento en dicha seguridad, bajo la dirección del Comité de Dirección de Seguridad de la Información (**CDSI**), que (i) velará e impulsará el cumplimiento de la PSI y de su desarrollo normativo, (ii) promoviendo la mejora continua en la gestión de la seguridad de la información y la protección de datos personales, y (iii) el seguimiento del estado de la política de continuidad del negocio e impulso de su mejora. A su vez, la presidencia de dicho Comité corresponde (artículo 6 de la Orden) a la persona titular de la Subsecretaría del Ministerio de Hacienda.

Por su parte, el Grupo de Trabajo Técnico de Seguridad de la Información (artículo 7 de la Orden), dependerá del CDSI, y será competente, con carácter permanente, para conocer las cuestiones técnicas que deban abordarse en relación con la PSI.

De acuerdo con lo dispuesto tanto en el preámbulo de la orden, como en su parte dispositiva, los miembros de la estructura organizativa de la gestión de seguridad, enumerados en el artículo 5, deberán cumplir las disposiciones establecidas en el ENS y en la normativa sobre protección de datos cuando el sistema de información se encuentre dentro del ámbito de aplicación de estas.

En lo que atañe a dicho Esquema y a la protección de datos de carácter personal, el preámbulo de la norma dispone que *“el Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS en el ámbito de la Administración Digital, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas. La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS. Del mismo modo, determina que **la Política de Seguridad de la Información debe ser coherente con lo establecido en el Reglamento (UE) 2016/679**, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos) y la normativa vigente en esta materia, en lo que corresponda, **prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.**”* (la negrita es nuestra)

*“La Política de Seguridad de la Información debe 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 la normativa vigente en esta materia, **prevaleciendo éstos en lo relativo a la protección de datos de carácter personal en caso de discrepancias.**”* (la negrita es nuestra)

Dichas normas se citan igualmente en los artículos 3 y 4, relativos, respectivamente, al marco legal y regulatorio, y a los principios de la seguridad de la información.

De ahí que el artículo **4.1 d)** establezca, dentro de los principios básicos de la seguridad de la información —siguiendo en este punto lo establecido en los artículos 5. b) y 7 del Esquema nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo)—, el de gestión de riesgos.

De acuerdo con dicho precepto:

*“El análisis y gestión de riesgos será parte esencial del proceso de seguridad. 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 establecerá 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. **El análisis y gestión de riesgos, cuando se aplique al tratamiento de datos personales, tendrá especial consideración con los riesgos para los derechos y libertades de las personas físicas.**”* (la negrita es nuestra)

Por su parte, en el artículo 14 del proyecto se desarrolla la metodología de dicho proceso de gestión de riesgos —con pleno sometimiento a la normativa de protección de datos—, así como la asignación de tareas entre los diferentes responsables del proceso. El citado sometimiento se explicita claramente en el citado artículo, cuando dispone:

*“1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que **evalúe los riesgos residuales y proponga tratamientos adecuados. Cuando el análisis de riesgos se aplique a tratamientos de datos personales, se tendrán en cuenta los riesgos posibles que afecten a los derechos y libertades de las personas físicas.*** (la negrita es nuestra)

*2. Cada órgano superior o directivo del Ministerio de Hacienda, así como cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, y siempre dentro de su ámbito de actuación y de sus competencias, se encargará de analizar y **evaluar los riesgos** de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas. (la negrita es nuestra)*

*3. Para la realización del **análisis de riesgos se tendrán en cuenta las recomendaciones publicadas** para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional y la **Agencia Española de Protección de Datos.**”* (la negrita es nuestra)

A mayor abundamiento, el artículo 16.2 —dentro de la regulación concreta relativa a “Protección de datos de carácter personal”—, señala que:

*“2. 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 el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos al **realizar la preceptiva evaluación de impacto** relativa a la protección de datos.”* (la negrita es nuestra)

Otras menciones destacadas sobre el cumplimiento de la normativa de protección de datos se obtienen *también* de las previsiones del **artículo 4.1** de la orden que se informa, cuando dispone:

*b) Responsabilidad diferenciada: (...) En los supuestos de tratamientos de datos personales además se identificará el responsable de tratamiento y, en su caso, el encargado de tratamiento, de acuerdo con el artículo 12 de esta Orden.*

*(...)*

*g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad y protección de datos personales por defecto y desde el diseño.*

Asimismo, en el artículo **4.2 a)** de la orden se configura como principio particular, el de *protección de datos de carácter personal*, indicando que:

*“a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que la seguridad del tratamiento es conforme con la normativa vigente en materia de protección de datos personales.”*

A su vez, en relación con el tratamiento de datos de carácter personal, el artículo 16 de la orden prevé que *(i)* se implementen las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que, *(ii)* en el caso de que el análisis de riesgos determine medidas agravadas, las medidas derivadas del análisis de riesgos correspondan a las previstas para la protección de datos de carácter personal, y que *(iii)* las auditorías de seguridad previstas en el ENS incorporen la revisión de las medidas técnicas y organizativas de seguridad de los datos personales a las que se refiere el propio artículo 16 de la orden, a saber:

*“Artículo 16. Protección de datos de carácter personal.*

1. 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 al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. El cumplimiento de este principio corresponde al 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. Esta responsabilidad 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 de datos personales relacionada en el art. 3 de esta Orden y 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, **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 Esquema Nacional de Seguridad.** (la negrita es nuestra)

2. 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 el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

3. 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.”

Respecto de la anterior previsión —relativa a la adopción de medidas de seguridad agravadas derivadas de la aplicación de la normativa de protección de datos—, tal y como se viene señalando en los informes emitidos por esta Agencia (por todos el **Informe 170/2018**, de 12 de noviembre de 2018), debe recordarse que, sin perjuicio de la aplicación de las exigencias derivadas de cualquier norma de mayor rango, en el caso de que el análisis de riesgos determine la necesidad de **medidas agravadas** respecto a la normativa recogida en el Anexo II del ENS, **siempre deberán implementarse las medidas derivadas del análisis de riesgos en materia de protección de datos personales.**

Así, según se señaló y ahora se reitera:

“Con carácter previo a analizar la concreta cuestión que 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 a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa. Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva”.*

*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 deber 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 ENS deberán prevalecer sobre éstas últimas**, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.



Por tanto, **se considera favorablemente la previsión del artículo 16 de la orden**, cuando dispone que en el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo (del ENS), las medidas derivadas de dicho análisis serán las que deban implementarse en aras de la protección de datos de carácter personal, teniéndose pues en cuenta lo dispuesto en el art. 32 RGPD.

## II

En cuanto a la gestión de la seguridad en el Ministerio, se establece una estructura organizativa específica que incluye al Comité de Dirección de Seguridad de la Información (**CDSI**), al Grupo de trabajo Técnico de Seguridad de la Información, a los responsables de seguridad del Ministerio, a los responsables de la información, a los responsables del servicio, a los responsables del sistema, y al delegado de protección de datos del departamento y las personas delegadas de Protección de Datos de los organismos públicos adscritos al mismo —*ex artículo 5*—.

Además de las funciones del CDSI y del Grupo de Trabajo Técnico de Seguridad de la Información (GTTSI), dependiente del CDSI, que —*ut supra*— quedaron ya expuestas, los responsables de seguridad son las personas que adoptarán las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, los responsables de la información y del servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos del servicio en materia de seguridad y, por tanto, la potestad de determinar los niveles de seguridad, y el responsable del sistema tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

En cuanto al delegado de protección de datos, su naturaleza y funciones se regulan en el artículo 11 del proyecto de orden de forma que esta Agencia considera mejorable, si se compara con otras órdenes PSI de otros departamentos ministeriales ya informadas. En consecuencia, **resulta necesario recordar** la labor de asesoramiento y supervisión que deberá ejercer dicho delegado en el ámbito de la orden que se informa, prestando asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica.

La enumeración de las funciones de los delegados de protección de datos se encuentra detallada 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 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Según se dispone en dichas normas, los delegados deberán ser nombrados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y en la práctica en materia de protección de datos, y a su capacidad para desempeñar las funciones que tienen encomendadas.

Sin embargo, el citado artículo 11 de la orden que se informa *se limita a señalar* que la designación del delegado se realizará de acuerdo con la normativa de protección de datos, siendo su figura *“única para todo el Departamento, sin perjuicio de la existencia de personas delegadas de Protección de Datos en los organismos públicos adscritos al Departamento y del nombramiento de coordinadoras o coordinadores en todos los órganos superiores del Departamento y en la Intervención General de la Administración del Estado.”*

Por ello, se sugiere que en la orden se señale que la designación del delegado se efectúe de conformidad con lo dispuesto por la legislación aplicable en materia de protección de datos, especialmente en atención a la regulación del artículo 37 del RGPD y del artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre.

Se sugiere que la redacción podría ser más completa, y a título de mera posibilidad, se propone la siguiente (con las adaptaciones que sean oportunas a las denominaciones de los órganos del departamento):

### **Artículo 11. Delegado de Protección de Datos**

*1. La persona Delegada de Protección de Datos, designado en virtud de lo dispuesto en los apartados 1 s) y 2 e) del artículo 13 del Real Decreto 206/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda, y de conformidad con los requisitos establecidos en el Reglamento General de Protección de Datos (Reglamento UE 2016/679), especialmente su art. 37, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, especialmente su art. 34, es única para todo el Departamento, sin perjuicio de la existencia de personas Delegadas de Protección de Datos, organismos públicos adscritos al Departamento y del nombramiento de coordinadoras, o coordinadores en todos los órganos superiores del Departamento y en la Intervención General de la Administración del Estado.*

*2. En el ámbito de los tratamientos de datos personales, y sin perjuicio de las atribuciones establecidas en el*

*Reglamento UE 2016/679 de forma exclusiva a los responsables y encargados de los tratamientos de datos personales, y de las atribuciones exclusivas de los Responsables de la Seguridad, el Delegado de Protección de Datos ejercerá labores de asesoramiento y supervisión en el ámbito de la presente norma.*

*3. Prestará asistencia y asesoramiento a los responsables del tratamiento, a la hora de identificar los riesgos y adoptar medidas para la protección de los datos personales, y en cuanto a la supervisión de que las mismas se han adoptado y llevado a la práctica. En cualquier caso, las funciones ejecutivas de toma de las decisiones oportunas al respecto serán responsabilidad de los respectivos responsables del tratamiento.*

*4. Ejercerá labores de asistencia y asesoramiento a los responsables del tratamiento de datos personales, a los Responsables de la Seguridad y a los responsables del Sistema, en los procesos de gestión de brechas de datos personales en el ámbito de la gestión general de incidentes de seguridad.*

*5. Prestará asesoramiento a los Responsables de la Seguridad y a los Responsables del Sistema, en cuanto a la implantación de medidas de seguridad que tengan un objeto distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales, tal y como dispone el artículo 24 del Real Decreto 311/2022, de 3 de mayo.*

*6. Participará en el CSSI en materia de protección de datos personales, en el compartido objetivo de procurar:*

- a) Alinear las respectivas normativas de cumplimiento, así como la definición e implantación de medidas de seguridad.*
- b) Impulsar y/o coordinar auditorías y revisiones del estado de cumplimiento de los requisitos y principios de la legislación aplicable.*
- c) Diseñar planes de formación y concienciación conjuntos con los de seguridad de la información.*

### III

A su vez, en relación con la *compatibilidad funcional del delegado de protección de datos del RGPD* (artículo 11) y el *responsable de seguridad* del Esquema Nacional de Seguridad (artículo 8), tal y como se indicó en el **Informe 170/2018**, **la orden deslinda claramente los ámbitos de actuación de ambas figuras.**

Por otro lado, resulta esencial diferenciar al delegado de protección de datos de la figura del propio responsable del tratamiento, bien con carácter general, bien en el sentido de la estructura organizativa que tendrá a su cargo el cumplimiento de las obligaciones impuestas por la normativa de protección de datos.

En el proyecto de orden las figuras del responsable y del encargado del tratamiento, se regulan —con absoluta independencia del delegado— en el artículo 12 de la orden.

El RGPD es claro a la hora de imponer al responsable la obligación de cumplimiento de las medidas que el mismo prevé. Será así el responsable quien deberá mantener un registro de operaciones de tratamiento, evaluar el riesgo concurrente en un determinado tratamiento de datos o desarrollar en su caso la evaluación de impacto exigida por el reglamento. Del mismo modo, será quien habrá de determinar las medidas técnicas y organizativas que hayan de adoptarse para garantizar la seguridad del tratamiento. Lógicamente, estas medidas se desarrollarán por quienes las tienen atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos y grupos enumerados en los artículos 6 a 10 del proyecto de orden, y, particularmente, el responsable de seguridad.

La función del delegado de protección de datos es la de prestar al responsable la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas y supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el delegado de protección de datos 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 del responsable del tratamiento, no del DPD.

Dado que se ha sugerido una propuesta de redacción del art. 11, las funciones del Delegado de Protección de datos previstas en dicho texto atribuidas al delegado encajarían claramente con su función prevista en el RGPD de asesoramiento y consulta, así como en el ámbito de sus relaciones con el resto de los órganos del responsable, puesto que, de otra parte, corresponde al delegado 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.

En lo relativo a su participación en las reuniones del “Comité de Dirección de Seguridad de la Información”, cuyas funciones se encuadran en el artículo 6 de la orden que se informa, su papel y funciones deberán desarrollarse únicamente en calidad de *invitado*.

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 el citado Comité 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 dicho Comité 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. A estos efectos, resulta acertada la previsión del artículo 6.1. 6º de la orden cuando dispone que dentro de la composición del CDSI, se encontrará:

*“La persona designada delegada de Protección de Datos del departamento, que participará con voz, pero sin voto, haciéndose constar en acta su parecer si no coincide con la decisión adoptada por el CDSI.”*