

0020/2025

## I

Tal y como dispone el artículo 1 del texto sometido a informe, constituye su objeto la aprobación de la Política de Seguridad de la Información —**PSI**— en el ámbito del Ministerio de Educación, Formación Profesional y Deportes, así como el establecimiento de la estructura para el gobierno y la gestión de la Seguridad de la Información, que serán de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio, incluidos los órganos dependientes o adscritos al mismo. Esta Política es aplicable a todos los activos de información empleados, y 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.

Por su parte, el Real Decreto 311/2022, de 3 de mayo, 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.

De este modo, el artículo 4 del proyecto regula los principios de la seguridad de la información, así como los objetivos que garantizan su cumplimiento. Igualmente, el artículo 5 desarrolla la estructura organizativa del Departamento en relación con la seguridad de la información, bajo la dirección del Comité de Dirección de Seguridad de la Información (CDSI), que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del ministerio (artículo 6 de la Orden). Por su parte, el Comité Operativo de Seguridad de la Información (COSI) —artículo 7—, creado en el seno del Comité de Dirección de Seguridad de la Información, y presidido por el titular de la Subdirección de Tecnologías de la Información y Comunicaciones, será el órgano encargado de coordinar técnicamente la seguridad de la información en el Departamento. Entre sus principales funciones se encuentran la revisión técnica de la seguridad, la evaluación de incidentes, la elaboración de normativa de seguridad de tercer y cuarto nivel, así como la coordinación con el Centro Criptológico Nacional, todo ello con el fin de garantizar el cumplimiento de la Política de Seguridad de la Información y fomentar la cultura de seguridad en la organización.

## II

En lo que atañe a la protección de datos de carácter personal, el preámbulo de la norma dispone que *“Dentro de ese marco legal cabe subrayar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Dicha ley orgánica adapta al ordenamiento jurídico español 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”*.

La normativa de protección de datos plantea nuevos retos, así como la necesidad de dar un nuevo enfoque al tratamiento de datos de carácter personal. De este modo, para garantizar su adecuada implantación resulta necesario intensificar la labor de coordinación con el resto de las normas de implantación obligatoria en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas. Dichas normas se enumeran de forma detallada en el artículo 3 de la Orden, relativo al marco legal y regulatorio, desarrollándose su contenido en los principios de la seguridad de la información de su artículo 4.

En este sentido, el artículo **4.1 e)** establece, dentro de los principios básicos de la seguridad de la información —siguiendo en este punto lo dispuesto en los artículos 5. b) y 7 del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo)—, el de “Análisis y gestión basada en los riesgos”:

De acuerdo con dicho precepto:

*“e) Análisis y gestión basada en los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. Se llevará a cabo una gestión de los riesgos que recoja un proceso de identificación, análisis, evaluación y tratamiento en los que los sistemas estén expuestos, lo que 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 y una proporcionalidad entre el valor y 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. **En el caso de que un sistema de la información realice tratamiento de datos personales, se realizará el análisis de riesgos y la evaluación de impacto, si así fuese necesario, según lo establecido en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en colaboración con la figura del Delegado de Protección de Datos**”.* (la negrita es nuestra)

A su vez, el artículo 4, 2. letra o), dentro de las directrices fundamentales de seguridad que deben orientar la actuación del Departamento, señala que:

*o) El Ministerio, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, **y de acuerdo con la normativa sobre protección de datos personales**, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los usuarios, reteniendo la **información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados**, la organización podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de **seguridad de la información**, de forma que sea posible **impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada** de código dañino así como otros daños a las antedichas redes y sistemas de información.* (la negrita es nuestra)

Por su parte, en los artículos 13 y 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, e incluso **prevalencia de lo previsto en la normativa de protección de datos**, se explicita claramente en el citado artículo 14, que, bajo el título, “Gestión de riesgos y protección de datos de carácter personal”, dispone:

*“Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Educación, Formación Profesional y Deportes **las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, de acuerdo a lo establecido por la Ley Orgánica 3/2018, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, y el Anexo II del Esquema Nacional de Seguridad**”.* (la negrita es nuestra)

Asimismo, en relación con el cumplimiento de las medidas de seguridad, el **artículo 4.2. n)** de la orden que se informa, dispone:

*“n) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento del marco legal vigente en materia de seguridad de la información, especialmente en lo relativo a la protección de datos de carácter personal”.*

### III

Según se ha expuesto, en relación con el tratamiento de datos de carácter personal, los artículos **4.1. e)** y **14** de la orden prevén que 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 se detalla en el RGPD y en la LOPDGDD, por lo que se impone la obligación de que, en el caso de que el análisis de riesgos determine medidas agravadas respecto a las que, además, hayan de aplicarse conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, las medidas derivadas del análisis de riesgos a implantar serán las derivadas de la normativa de protección de datos de carácter personal.

Pues bien, dicha previsión, que responde a lo establecido en el art. 3.3 del citado Real Decreto 311/2022, 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 la previsión de los artículos 4.1. e) y 14** de la Orden sometida a informe, de los que se desprende 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 en cuenta lo dispuesto en el artículo 32 del RGPD relativo a la “Seguridad del Tratamiento”.

#### **IV**

En cuanto a la gestión de la seguridad en el Ministerio, se establece en el art. 5 del Proyecto una estructura organizativa específica que incluye al Comité de Dirección de Seguridad de la Información (CDSI), al Comité Operativo de Seguridad de la Información (COSI), al Responsable de Seguridad, a los Responsables de la Información, a los Responsables del Servicio, y a los Responsables del Sistema de Información, así como al Delegado de Protección de Datos designado por la Subsecretaría, y al resto de Delegados de Protección de Datos de los organismos dependientes que se adhieran a la PSI, **lo cual se considera asimismo favorablemente.**

El Comité de Dirección de Seguridad de la Información (CDSI), adscrito a la Subsecretaría en el marco de la Comisión Ministerial de Administración Digital, es el órgano colegiado encargado de coordinar y gestionar la seguridad de los sistemas de información. Su labor incluye actualizar la política de seguridad, supervisar su cumplimiento, resolver conflictos, ordenar auditorías, promover la formación en seguridad, y apoyar la mejora continua, pudiendo delegar funciones y recabar asesoramiento técnico o externo para fundamentar sus decisiones.

Por su parte, el Comité Operativo de Seguridad de la Información (COSI), de carácter permanente y creado dentro del CDSI, se encarga de abordar las cuestiones técnicas relativas a la seguridad de la información y coordinar su gestión en todo el Departamento y con otros órganos de la Administración General del Estado. Presidido por el titular de la Subdirección de Tecnologías de la Información y Comunicaciones, reúne a representantes clave del Ministerio y asume funciones técnicas como dirigir revisiones, evaluar incidentes, elaborar normativa, establecer indicadores, coordinar con el Centro Criptológico Nacional y fomentar la conciencia de seguridad, reuniéndose de forma trimestral o extraordinaria según lo determine su presidente.

El Responsable de Seguridad, asumido por el titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, es quien toma decisiones para garantizar la seguridad de la información y de los servicios, asegurando que los comités competentes aborden las necesidades relevantes en cada momento. En el marco del sistema de gestión de seguridad, sus funciones incluyen mantener y verificar medidas de protección, supervisar incidentes, elaborar informes, fomentar la formación, realizar análisis de riesgos, promover auditorías y gestionar la documentación normativa, contando para ello con un equipo operativo encargado de la gestión de incidentes y de la continuidad de los sistemas críticos.

*Los Responsables de la Información y del Servicio* son los encargados de definir los requisitos de seguridad aplicables a la información y los servicios bajo su competencia, actuando, además, en el caso de los primeros, como responsables del tratamiento de datos personales. Estas funciones recaen en los titulares de los órganos o unidades administrativas que gestionan procedimientos, pudiendo una misma persona asumir ambos roles, los cuales suelen recaer en personas físicas u órganos colegiados que forman parte del CDSI. Y, finalmente, el Responsable del Sistema se encarga de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, siendo designado por cada órgano superior del Departamento según su estructura interna.

En cuanto al Delegado de Protección de Datos —DPD—, su naturaleza y funciones se regulan en el artículo 11 del proyecto de Orden. Desempeñará las funciones establecidas en la normativa nacional y europea sobre protección de datos, y su designación en el Ministerio y organismos adheridos se basará en su cualificación profesional, experiencia y conocimientos jurídicos, notificándose su nombramiento al Responsable de Seguridad.

A este respecto, teniendo en cuenta la regulación general de la figura del DPD —cuyas funciones se contienen 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—, este **deberá ejercer las labores de asesoramiento y supervisión 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.**

A su vez, debe reiterarse que, en consonancia con lo previsto en la Orden que se informa, la designación del delegado debe efectuarse 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.

En consecuencia, dichos delegados deberán ser nombrados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos, y a su capacidad para desempeñar las funciones que tienen encomendadas.

## **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 5 —referido a la estructura organizativa—, y 11 de la Orden —en relación con el Delegado de Protección de Datos—, respeta el esencial conocimiento que este debe poseer de la política de seguridad de la información, participando con su asesoramiento en su implantación en virtud de las funciones que le otorga expresamente el RGPD.

A su vez, en relación con 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 diferenciar al DPD de la figura del *Responsable* del tratamiento —según se infiere claramente del artículo 9.1 segundo inciso del proyecto— que tendrá a su cargo el *cumplimiento de las obligaciones impuestas por la normativa de protección de datos*, a saber:

“Artículo 9. Los Responsables de la Información y los Responsables del Servicio

1. Los Responsables de la Información y los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de los servicios y de la información que manejan. A los efectos previstos en el marco legal de protección de datos de carácter personal, **los Responsables de la Información tendrán asimismo la consideración de responsables del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación.** (la negrita es nuestra)

En este sentido, el RGPD es claro a la hora de imponer al Responsable del tratamiento la obligación de cumplir 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 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 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.

Sin embargo, en lo relativo a su *posible* 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, en su caso (cuando dicha composición del CDSI se regule por la *futura* Orden ministerial de creación y regulación de la Comisión Ministerial de Administración Digital del Departamento —CMAD—), su papel y funciones deberán desarrollarse únicamente en calidad de *invitado*.

Idéntico papel y funciones deberán considerarse en cuanto a su participación en las reuniones del Comité Operativo de Seguridad de la Información —COSI—, del artículo 7 de la Orden sometida a informe, cuando señala que el DPD participará en las reuniones de dicho COSI.

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 comités 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 expuso 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, y en el 36/2024 respecto a la PSI del Ministerio de Inclusión, Seguridad Social y Migraciones.

Finalmente, en cuanto a la redacción del artículo 14 del proyecto de Orden, se sugiere añadir la expresión “técnicas y organizativas” a la expresión “de seguridad”, que ya se contiene. De este modo, el precepto se referirá claramente a las medidas técnicas y organizativas previstas en los artículos 24 y 32 del RGPD, proponiéndose la siguiente redacción u otra similar:

*Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Educación, Formación Profesional y Deportes **las medidas técnicas y organizativas, así como de seguridad** apropiadas derivadas del análisis de riesgos, y de la evaluación de impacto relativa a la protección de datos, de acuerdo a lo establecido por la Ley Orgánica 3/2018, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, y el Anexo II del Esquema Nacional de Seguridad. (la negrita es nuestra)*

## VI

**En conclusión**, el proyecto de Orden analizado cumple con las exigencias normativas en materia de protección de datos personales, al prever expresamente 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 Reglamento General de Protección de Datos —RGPD— y a la Ley Orgánica 3/2018, de 5 de diciembre. Además, se garantiza el respeto a los principios fundamentales de protección de datos, como la limitación de finalidad, la minimización de datos y la limitación del plazo de conservación.

Asimismo, los artículos 13 y 14 del proyecto desarrollan 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. Se establece que las medidas derivadas del análisis de riesgos previstas en el artículo 32 del RGPD, cuando resulten más estrictas que las del Esquema Nacional de Seguridad, deberán prevalecer sobre estas últimas para garantizar el cumplimiento adecuado del Reglamento.

Por último, se recuerda 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.

**Todo lo anterior se encuentra debidamente contemplado en el proyecto de orden que se informa.**

**La única enmienda** que se sugiere se refiere a la redacción del artículo 14 del proyecto de Orden, proponiéndose añadir la expresión “técnicas y organizativas” a la mención actual a las “medidas de seguridad”, de modo que el precepto haga referencia expresa a las medidas previstas en los artículos 24 y 32 del RGPD. En concreto, **se sugiere la siguiente redacción** u otra similar:

*“Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Educación, Formación Profesional y Deportes **las medidas técnicas y organizativas, así como de seguridad apropiadas** derivadas del análisis de riesgos, y de la evaluación de impacto relativa a la protección de datos, de acuerdo a lo establecido por la Ley Orgánica 3/2018, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, y el Anexo II del Esquema Nacional de Seguridad.”* (la negrita es nuestra)