

0036/2024

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 el ámbito del Ministerio de Inclusión, Seguridad y Migraciones, 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.

Así, 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 desarrolla los principios de la seguridad de la información, así como los objetivos que garantizan su cumplimiento. Igualmente se desarrolla la estructura organizativa del Departamento en relación con la seguridad de la información, bajo la dirección del Comité de Seguridad de los Sistemas de Información (**CSSI**), que coordinará todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del ministerio (artículo 7 de la Orden). A su vez, el responsable del sistema global de información (artículo 6 de la Orden) —que es el titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones—, será el responsable último del funcionamiento de los servicios, cuya principal misión será hacer cumplir las disposiciones establecidas en el Esquema Nacional de Seguridad 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 la protección de datos de carácter personal, el preámbulo de la norma dispone 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, 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)

De tal modo, continúa la exposición de motivos, 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 obligatoria implantación en la organización, especialmente con el Esquema Nacional de Seguridad, buscando sinergias en el desarrollo de ambas.*” 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 los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción a 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. **Además, las medidas de seguridad deberán garantizar el cumplimiento de lo previsto en el artículo 32 del RGPD, por lo que el responsable del tratamiento de datos personales, y en su caso, de los encargados del tratamiento, podrán adoptar todas aquellas medidas adicionales con el fin de garantizar la seguridad de los datos personales, en virtud de lo dispuesto en el artículo 24 y 25 del RGPD, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, y en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.**”* (la negrita es nuestra)

Por su parte, en los artículos 13 y 15 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 15, que, bajo el título, “Protección de datos de carácter personal”, dispone:

*“1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del MISSM, 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 Ley Orgánica 3/2018, de 5 de diciembre. (la negrita es nuestra)*

*Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo. **En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.** (la negrita es nuestra)*

*En particular, **se tendrá en cuenta el artículo 32 del RGPD**, en cuanto a la exigencia de una identificación de riesgos específicos para los derechos y libertades de las personas en relación a los tratamientos de datos personales, que debe ser previo al análisis de riesgos de los sistemas donde se implementen dichos tratamientos, de forma que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos personales suponen para los derechos y libertades de las personas. (la negrita es nuestra)*

2. Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos Responsables de los Sistemas, podrán implementar tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto que la protección de los datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022 (...).

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 se identificará además a la persona, organismo o unidad responsable de tratamientos y, en su caso, al encargado de tratamiento, de acuerdo con las definiciones del artículo 4, apartados 7 y 8, del RGPD.” (...)*

***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. Además, con el fin de garantizar la resiliencia y la protección de los*

datos personales, se deben tener en cuenta las medidas de seguridad por defecto en base a los artículos 24 y 25 del RGPD, así como las medidas de seguridad orientadas al riesgo según el artículo 32 del RGPD.

h) Vigilancia continua: (..) En cuanto la gestión de incidentes que afecten a datos personales, se tendrá en cuenta las obligaciones específicas de notificación, comunicación y documentación especificadas en los artículos 33 y 34 del RGPD.”

Asimismo, en el artículo 4.2 a) de la orden se configura como principio particular y responsabilidad específica, 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 el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.”

Según se ha expuesto, en relación con el tratamiento de datos de carácter personal, el artículo 15 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 se detalla en el RGPD y en la LOPDGDD, y que, (ii) en el caso de que el análisis de riesgos determine medidas agravadas respecto a las que, además, hayan de aplicarse conforme al Anexo II del 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 serán las que se implementarán en la 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, ha venido siendo señalada 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 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 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.

Por tanto, **se considera favorablemente la previsión del artículo 15 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 en cuenta lo dispuesto en el artículo 32 del RGPD.

II

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 responsable del sistema global de información, al Comité de Seguridad de los Sistemas de Información (**CSSI**), a los responsables de los sistemas de información, a los responsables de seguridad del Ministerio, y al responsable de la prestación del servicio, así como al Delegado de Protección de datos, lo cual se considera asimismo favorablemente, por las razones ya expresadas en el epígrafe anterior.

El responsable del sistema global de información es el titular de la Subsecretaría de Inclusión, Seguridad Social y Migraciones, y tiene la responsabilidad última del funcionamiento de los servicios y de integrar todos los sistemas de información de los órganos superiores y directivos y unidades dependientes del Ministerio.

Por su parte, el CSSI coordina todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del Ministerio, pudiendo asumir las funciones de Responsable del Sistema de Información y Responsable de la Prestación del Servicio cuando así lo decida.

Los responsables de sistemas de información tienen la responsabilidad de poner en marcha, mantener y actualizar las medidas de seguridad pertinentes en sus respectivos ámbitos. Esto incluye determinar los requisitos de seguridad de la información tratada, de los tratamientos realizados sobre la misma y de los servicios electrónicos prestados. Estos responsables son los titulares de todos los órganos superiores y directivos del Ministerio y de todos los organismos adscritos y órganos dependientes.

El responsable de la prestación del servicio tiene la obligación de implementar las medidas de seguridad sugeridas por el responsable de seguridad e incluidas en el plan director de seguridad. Finalmente, el responsable de seguridad del Ministerio tiene la responsabilidad de determinar las decisiones para satisfacer los requisitos de seguridad de la información, de los tratamientos, y de los servicios electrónicos. Al titular de dicho puesto se le garantiza la debida independencia en el ejercicio de sus funciones, y debe asistir al delegado de protección de datos en cuestiones relativas a la seguridad de los sistemas de información.

En cuanto al delegado de protección de datos, su naturaleza y funciones se regulan en el artículo 11 del proyecto de orden. Dicho delegado ejercerá 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. La enumeración de sus funciones coincide con la 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.

El delegado de protección de datos también participará en el CSSI en materia de protección de datos personales, alineando las normativas de cumplimiento, coordinando auditorías y revisiones del estado de cumplimiento, y diseñando planes de formación y concienciación.

A este respecto, debe recordarse que 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 tiene encomendadas.

Además, el art. 12 del proyecto configura a los responsables y encargados de los tratamientos de datos personales de la misma manera que lo hace el RGPD y la LOPDGDD.

III

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 el **Informe 170/2018 citado**, **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, -lo que recuerda adecuadamente el art. 11.3 segundo inciso del proyecto- 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 este sentido, el RGPD es claro a la hora de imponer al responsable del tratamiento 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 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 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 en su función de asesoramiento y consulta, así como en el ámbito de sus relaciones con el resto de los órganos del responsable. Asimismo, el delegado 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 participación en las reuniones del “Comité de Seguridad de los Sistemas de Información”, cuyas funciones se encuadran en el artículo 7 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.

Así se expuso ya en el Informe 85/2022 de esta AEPD, y más específicamente en el 103/2022, relativo a la PSI del Ministerio de Trabajo y Economía Social. Del mismo modo, el Informe del Delegado de Protección de Datos del actual Ministerio de Inclusión, presentado con la documentación remitida a esta AEPD sobre el Proyecto de Orden, sugiere que la participación de este en el CSSI lo sea “como asesor con voz pero sin voto o expresión similar”, lo que esta AEPD a su vez suscribe.

IV

Por lo demás, el art. 1.2 parece excepcionar -sin mayores explicaciones acerca de las razones de ello- la posible aplicación de esta PSI a la Secretaría de Estado de Seguridad Social y Pensiones, y las entidades gestoras y servicios comunes de la Administración de la Seguridad Social adscritas a la misma. Ello, como es obvio, en ningún caso puede entenderse que supone una excepción de estos órganos o entidades a la aplicación de la normativa de protección de datos que en cada caso les sean aplicables. En el art. 4.2, letra e) se recoge que *“Para proteger las redes del Departamento, se analizará el tráfico cifrado de usuarios de forma automatizada. Se realizará la excepción en este análisis de las categorías de navegación relacionadas con datos sensibles especialmente protegidos de acuerdo con la normativa de protección de datos vigente, siempre que sea posible la discriminación”*. Esto es, dice que se analizará el tráfico cifrado de los usuarios, salvo el que conlleve “datos sensibles especialmente protegidos”, “siempre que sea posible la discriminación”, lo que conlleva que cuando no sea posible, también se “analizará” el tráfico que conlleve datos sensibles. Pues bien, dicho “análisis” de “datos sensibles”, cuando se produzca, será un verdadero tratamiento de datos personales, que conforme al art. 9 RGPD está, en principio, prohibido, salvo que concurra alguna de las causas que levantan la prohibición prevista en el art. 9.2 RGPD, amén de contar con alguna de las bases jurídicas previstas en el art. 6.1 RGPD. Ello quiere decir que para tratar dichos datos “sensibles”, el responsable del tratamiento habrá de contar con dicha causa que levante la prohibición en el tratamiento y con la correspondiente base jurídica, y explicitar todo ello en el Registro e Inventario de actividades de tratamiento.

En el primer apartado del art. 15, para que el precepto haga referencia tanto a las medidas técnicas y organizativas previstas en el art. 24 como a la misma expresión que se contiene en el art. 32, ambos del RGPD, se sugiere añadir la expresión “técnicas y organizativas” a la expresión “de seguridad”, que ya se contiene, de la siguiente manera:

*1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del MISSM, **las medidas técnicas y organizativas así como 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 Ley Orgánica 3/2018, de 5 de diciembre.*