

0027/2025**I**

El proyecto de Orden tiene por objeto la aprobación de la Política de Seguridad de la Información (PSI) en el ámbito del Ministerio de Derechos Sociales, Consumo y Agenda 2030, tal y como establece su artículo 1. Esta política, cuyo contenido se desarrolla en el articulado y en el ANEXO del texto que se informa, recoge las directrices que rigen la gestión y protección de la información tratada y de los servicios prestados por el Ministerio en el contexto de la Administración Electrónica.

Asimismo, la Orden establece la estructura organizativa necesaria para definir, implantar y gestionar la PSI. En particular, la Cláusula Decimoquinta del ANEXO define los tres niveles normativos sobre los que se articula esta política, con el objetivo de conformar un marco normativo común aplicable a todos los órganos incluidos en su ámbito de aplicación.

En este sentido, debe recordarse que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad —ENS— en su artículo 12.3, prevé que *“En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento”*, disponiéndose en el apartado 6 del propio artículo 12, que la política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los requisitos mínimos que en dicho Esquema Nacional se contemplan. Por otra parte, esta **PSI** se dirige a garantizar el debido cumplimiento de lo dispuesto en la normativa de protección de datos.

En la orden que se informa, la **Cláusula Tercera** de su ANEXO define la misión del Ministerio de Derechos Sociales, Consumo y Agenda 2030, de acuerdo con el Real Decreto 209/2024, de 27 de febrero, estableciendo su responsabilidad en la propuesta y ejecución de las políticas del Gobierno en materia de derechos sociales, bienestar y diversidad familiar, atención a la dependencia y discapacidad, protección de los animales, consumo, regulación del juego, así como en el impulso y seguimiento de la Agenda 2030 y los Objetivos de Desarrollo Sostenible.

La **Cláusula Quinta** regula los principios de la seguridad de la información, conforme a lo previsto en el Real Decreto 311/2022, de 3 de mayo, sobre los cuales se implantan medidas de seguridad proporcionales a los riesgos y al valor de la información y los servicios. Estos principios incluyen: el compromiso estratégico de toda la estructura organizativa, el enfoque integral y continuo basado en riesgos, la implantación de medidas de prevención, detección y respuesta, la existencia de múltiples líneas de defensa, la vigilancia permanente, la asignación diferenciada de responsabilidades, la proporcionalidad de las medidas adoptadas y la incorporación de la seguridad desde el diseño y por defecto, en consonancia también con lo dispuesto en el Reglamento General de Protección de Datos (RGPD).

Por su parte, la **Cláusula Sexta** desarrolla la estructura organizativa del Ministerio en relación con la seguridad de la información, incluyendo los principales órganos y figuras responsables de su implantación y seguimiento. Entre ellos, destacan la Comisión Ministerial de Administración Digital (CMAD) y el Comité de Seguridad de la Información (CSI), así como los responsables de seguridad (RSeg), de la información (RInf), del servicio (RSer) y del sistema (RSis), quienes desempeñan funciones específicas en el marco de la Política de Seguridad de la Información para garantizar su correcta aplicación, mantenimiento y evolución.

II

En lo que atañe a la protección de datos de carácter personal, el artículo 2 de la Orden dispone que:

“Artículo 2. Protección de datos de carácter personal.

1. El tratamiento de datos de carácter personal en el ámbito del Ministerio de Derechos Sociales, Consumo y Agenda 2030 se efectuará **conforme a los principios** de licitud, transparencia y lealtad, finalidad, minimización, exactitud, limitación del plazo de conservación, integridad y confidencialidad, así como responsabilidad proactiva y seguridad. (la negrita es nuestra)

2. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de los órganos superiores y directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, además de sus organismos y entidades adscritas o dependientes, ya sean tratamientos automatizados o no automatizados, **las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos personales, conforme se detalla en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).** **Además,** en cumplimiento de la disposición adicional primera de la Ley

Orgánica 3/2018, de 5 de diciembre, **se aplicarán las medidas de seguridad correspondientes a la categoría del Sistema según el anexo II del 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. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 3/2010 de 8 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.** (la negrita es nuestra)

3. En relación con los sistemas de información que, para soportar la prestación de servicios de administración electrónica, manejen datos de carácter personal, **prevalecerán las mayores exigencias contenidas en la normativa de protección de datos en vigor** que afecte al sistema de información concreto.

4. 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.

5. **Corresponde al delegado** de Protección de Datos (DPD) del Ministerio de Derechos Sociales, Consumo y Agenda 2030 **informar y asesorar a los Responsables del Tratamiento de las obligaciones que les incumben en virtud del RGPD, además de supervisar** el cumplimiento de la normativa en materia de protección de datos de carácter personal del departamento, ofrecer **asesoramiento y actuar como interlocutor de los Responsables del Tratamiento con la Agencia** Española de Protección de Datos. (la negrita es nuestra)

En consecuencia, en relación con el tratamiento de datos de carácter personal, el artículo 2 de la orden prevé el pleno sometimiento de los tratamientos de datos realizados, tanto a los principios de protección de datos, como a las medidas de seguridad técnicas y organizativas reguladas en la normativa de protección de datos. Dichas medidas de seguridad apropiadas en cada caso, y derivadas del análisis de riesgos, así como la realización de una evaluación de impacto relativa a la protección de datos, según se detalla en el RGPD y en la LOPDGDD, se concretarán en determinadas **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.**

A su vez, el propio artículo 2, en su apartado 5, regula con la necesaria amplitud, la figura y funciones del Delegado de Protección de Datos del ministerio, en similares términos que los dispuestos 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.

Dicho Delegado 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 su puesta en práctica.

A su vez, debe reiterarse que, de acuerdo con la regulación general del artículo 37 del RGPD y del artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre, la designación del Delegado debe efectuarse de conformidad con lo dispuesto por la legislación aplicable en materia de protección de datos. En consecuencia, dicho delegado deberá ser nombrado 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.

En conclusión, conforme a lo expuesto, **se informa favorablemente el contenido del artículo 2 del proyecto de Orden objeto de análisis, dado que dicho precepto regula con la suficiente amplitud, y en coherencia con la normativa de protección de datos, las cuestiones relativas a esta materia en lo relativo a la realización de los tratamientos de datos derivados de lo establecido en la propia Orden.**

Muy especialmente, en relación con la adopción de **medidas agravadas** adoptadas a consecuencia del análisis de riesgos, dicha previsión —que responde a lo establecido en el art. 3.3 del Real Decreto 311/2022, de 3 de mayo—, 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 del artículo 2** de la Orden sometida a informe, en la que se prevé que, cuando el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el Anexo del Esquema Nacional de Seguridad —actualmente reguladas en el Real Decreto 311/2022, de 3 de mayo—, las medidas derivadas de dicho análisis serán las que deban implementarse en aras de la protección de datos de carácter personal (teniéndose así en cuenta lo dispuesto en el artículo 32 del RGPD relativo a la “Seguridad del Tratamiento”).

III

Por otra parte, la normativa de protección de datos plantea nuevos retos, así como la necesidad de ofrecer 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 regulaciones. Dichas normas se enumeran de forma detallada en la cláusula **Cuarta** del ANEXO de la Orden, relativo al marco normativo, desarrollándose su contenido en los principios de la seguridad de la información de su cláusula **Quinta**.

En este sentido, la cláusula **Quinta, letra c)** establece, dentro de los principios básicos de la seguridad de la información —siguiendo en este punto lo dispuesto en los artículos 5. b), 7 y 10 del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo)—, el de “Gestión de la seguridad basada en los riesgos”, que será parte esencial del proceso de seguridad, estableciendo un proceso formal para la gestión de los riesgos que permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables y se realizará de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos, vigilancia continua y reevaluación periódica (artículos 7 y 10 del Real Decreto 311/2022, de 3 de mayo).

A su vez, la cláusula **Quinta, letra i)**, dentro de dichas directrices fundamentales de seguridad, que deben orientar la actuación del Departamento, señala la adopción del principio de “Seguridad desde el diseño y por defecto”, en los siguientes términos:

“i) Seguridad desde el diseño y por defecto: La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de cualquier sistema de información. Por tanto, 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.**” (la negrita es nuestra)

Pues bien, la citada regulación —que supone una remisión expresa a la normativa de protección de datos en cuanto a la adopción de las correspondientes medidas de seguridad técnicas y organizativas—, resulta, asimismo, **plenamente conforme con la normativa de protección de datos, por lo que se informa favorablemente el contenido de dichas cláusulas.**

IV

En cuanto a la gestión de la seguridad en el Ministerio, se establece en la cláusula **Sexta** el desarrollo de su estructura organizativa en relación con la seguridad de la información, incluyendo los principales órganos y figuras responsables de su implantación y seguimiento. Entre ellos, destacan la Comisión Ministerial de Administración Digital (CMAD) y el Comité de Seguridad de la Información (CSI), así como los Responsables de Seguridad (RSeg), de la Información (RInf), del Servicio (RSer) y del Sistema (RSis), quienes desempeñan funciones específicas en el marco de la Política de Seguridad de la Información para garantizar su correcta aplicación, mantenimiento y evolución, **lo cual se informa asimismo favorablemente.**

La Comisión Ministerial de Administración Digital (CMAD) es el órgano colegiado encargado de impulsar y coordinar internamente la administración digital. En materia de seguridad, lidera la elaboración de la estrategia organizativa, supervisa el cumplimiento del Esquema Nacional de Seguridad, vela por la aplicación y actualización de la política de seguridad, aprueba planes de auditoría y formación, resuelve conflictos competenciales, y garantiza la asignación de roles y recursos adecuados. Además, puede recabar asesoramiento técnico y promueve la colaboración interadministrativa, compartiendo buenas prácticas y reportando al Comité de Seguridad de la Información.

Por su parte, el Comité de Seguridad de la Información (CSI) es el órgano colegiado responsable de coordinar y supervisar la seguridad de la información en el Ministerio. Ejerce las funciones del Responsable de Seguridad en los centros que no lo hayan designado expresamente, promueve la mejora continua, la continuidad del servicio y el cumplimiento normativo, y colabora estrechamente con la CMAD. Aprueba planes, procedimientos, políticas y controles, valida su implantación, coordina incidentes, auditorías y formación, y vela por la protección de datos personales. Puede crear grupos de trabajo, invitar expertos, delegar funciones y reportar periódicamente el estado de la seguridad.

El Responsable de Seguridad, es la figura encargada de asegurar que los sistemas de información y los servicios electrónicos del ministerio cumplan los requisitos de seguridad y protección de datos. Supervisa la implantación de medidas, promueve la mejora continua y reporta a la CMAD. Su actuación se limita a los sistemas y servicios bajo su responsabilidad directa. Se trata de una figura que debe ser independiente del Responsable del Sistema. Si por falta de recursos ambas funciones recaen en la misma persona o entre personas con jerarquía, se aplicarán medidas compensatorias para asegurar la separación de responsabilidades.

El Responsable de la Información es quien determina los requisitos de seguridad aplicables a la información tratada por la organización, incluyendo los niveles de seguridad en función de su confidencialidad, integridad y disponibilidad. Cuando la información contiene datos personales, debe aplicar las medidas del RGPD y puede ser considerado responsable o encargado del tratamiento, debiendo llevar el correspondiente registro de actividades. Su función incluye participar en los análisis de riesgos, aceptar los riesgos residuales y solicitar informe al Responsable de Seguridad en determinadas ocasiones. Este rol puede coincidir con el del Responsable del Servicio si así lo permite la estructura organizativa, pero nunca con el del Responsable del Sistema.

El Responsable del Servicio establece y aprueba los requisitos de seguridad aplicables a la prestación de los servicios, siendo el máximo responsable de su funcionamiento y protección. Tiene capacidad para decidir sobre la finalidad y forma de prestación del servicio y participa también en el análisis de riesgos junto al Responsable de la Información y el de Seguridad. Puede coincidir con el Responsable de la Información cuando ambos recaen sobre la misma unidad, pero no podrá ejercer simultáneamente las funciones de Responsable de Seguridad ni de Responsable del Sistema, incluso en organizaciones pequeñas. Su designación corresponde a los órganos superiores del ministerio o sus organismos dependientes, sin que ello implique aumento de dotación ni retribución.

Y, finalmente, el Responsable del Sistema define e implementa la seguridad técnica del sistema de información y supervisa su funcionamiento, pudiendo delegar en personal bajo su responsabilidad. Este rol, designado por la CMAD, no puede coincidir con los de Información, Servicio ni Seguridad.

En cuanto al **Delegado de Protección de Datos** —DPD—, su naturaleza y funciones se regulan en el artículo 2.5 del proyecto de Orden, correspondiéndole informar y asesorar a los Responsables del Tratamiento de las obligaciones que les incumben en virtud del RGPD, además de supervisar el cumplimiento de la normativa en materia de protección de datos de carácter personal del departamento, ofrecer asesoramiento y actuar como interlocutor de los Responsables del Tratamiento con la AEPD.

Según se expuso anteriormente, la designación del Delegado en el Ministerio y organismos adheridos deberá basarse en su cualificación profesional, experiencia y conocimientos jurídicos, debiendo 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.

A este respecto, teniendo en cuenta la regulación general de la figura del **Delegado** —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—, **las previsiones del artículo 2.5 del proyecto de Orden, resultan conformes con la normativa de protección de datos, si bien ha de reiterarse 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.**

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 la **Cláusula Sexta y siguientes** —referidas a la organización de la seguridad—, y **artículo 2.5 de la Orden** —en relación con el Delegado de Protección de Datos—, respetan el esencial conocimiento que este debe poseer de la política de seguridad de la información, participando con su asesoramiento en su implantación en virtud de las funciones que le otorga expresamente el RGPD. A este respecto, de acuerdo con la **Cláusula Novena** del ANEXO, el Delegado puede asistir a las reuniones del Comité de Seguridad de la Información.

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

Por otro lado, resulta esencial identificar la figura del **Responsable del tratamiento** que —según se infiere claramente de la **Cláusula Quinta, letra g)** del ANEXO del proyecto— será la persona, organismo o unidad responsable del tratamiento y, en su caso, al **Encargado del Tratamiento**, de acuerdo con lo dispuesto en los apartados 7 y 8 del artículo 4 del RGPD.

“Cláusula Quinta, letra g:

“g) Diferenciación de responsabilidades: Se definirán los distintos roles intervinientes en los sistemas de información y se diferenciará: el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad de la información, que determina las decisiones para satisfacer los requisitos de seguridad. **En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado del tratamiento, de acuerdo con lo dispuesto en los apartados 7 y 8 del artículo 4 del RGPD.**” (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 las Cláusulas **Sexta a Duodécima** del ANEXO 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 Seguridad de la Información” —Cláusula **Novena**—, en su caso, su papel y funciones deberán desarrollarse únicamente en calidad de *invitado*. Asimismo, idéntico papel y funciones (“de invitado”) deberán considerarse en cuanto a su participación en las reuniones del resto de Comités y/o Comisiones establecidas en la Orden.

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

Así se 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, en el 36/2024 respecto a la PSI del Ministerio de Inclusión, Seguridad Social y Migraciones, y en el 20/2025 en relación con la PSI del Ministerio de Educación, Formación Profesional y Deportes.

En cuanto a la “Gestión de riesgos”, la **Cláusula Decimosexta** del ANEXO comprende una amplia y completa regulación, que resulta conforme con las previsiones tanto del Real Decreto 311/2022, de 3 de mayo, como con la normativa de protección de datos. Así, específicamente, en el apartado 8 de dicha Cláusula Decimosexta, se dispone que:

“Decimosexta. *Gestión de los riesgos*.

(...)

8. Los análisis de riesgos y de impacto, desde el enfoque relativo a la protección de datos especificado en RGPD, se realizarán según lo establecido en la normativa vigente en materia de protección de datos personales, debiendo seguir también las indicaciones de la Agencia Española de Protección de Datos y demás autoridades competentes al respecto.”

Finalmente, en cuanto a la redacción del **artículo 2.2** del proyecto de Orden, se sugiere añadir la expresión “técnicas y organizativas” a la expresión “medidas 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:

“2. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de los órganos superiores y directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, además de sus organismos y entidades adscritas o dependientes, ya sean tratamientos automatizados o no automatizados, las medidas de seguridad **técnicas y organizativas** apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos personales, conforme se detalla en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad correspondientes a la categoría del Sistema según el anexo II del 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. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 3/2010 de 8 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal. (la negrita es nuestra)

VI

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

Todas estas previsiones, así como el resto de las analizadas en el cuerpo del presente informe, se contienen en el artículo 2 del proyecto de Orden, que se refiere de manera específica al tratamiento de los datos de carácter personal.

Asimismo, la Cláusula Decimosexta del proyecto de Orden desarrolla detalladamente la metodología de gestión de riesgos y la asignación de responsabilidades, asegurando la prevalencia de la normativa de protección de datos en todo el proceso. Tanto el artículo 2 del proyecto como la citada

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

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 2.2 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:

*“2. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte de los órganos superiores y directivos del Ministerio de Derechos Sociales, Consumo y Agenda 2030, además de sus organismos y entidades adscritas o dependientes, ya sean tratamientos automatizados o no automatizados, las medidas de seguridad **técnicas y organizativas** apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos personales, conforme se detalla en el Reglamento (...)”* (la negrita es nuestra)

Finalmente, en lo relativo a la figura del **Delegado**, las previsiones del **artículo 2.5 del proyecto de Orden**, resultan conformes con la normativa de protección de datos, si bien ha de reiterarse 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.