

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

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 Asuntos Económicos y Transformación Digital.

En este sentido, el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad exige que cada administración pública cuente con una política de seguridad formalmente aprobada por el órgano competente. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Esta política de seguridad se establecerá de acuerdo con los principios básicos recogidos en el capítulo II de la propia norma (seguridad como proceso integral, gestión de la seguridad basada en riesgos, prevención, detección, respuesta y conservación, existencia de líneas de defensa, vigilancia continua, reevaluación periódica, y diferenciación de responsabilidades) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 12, en su apartado 6.

De este modo, el 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 Dirección de Seguridad de la Información, las directrices en materia de gestión de riesgos y los instrumentos normativos de la política de seguridad, conformados por tres niveles normativos estructurados jerárquicamente.

En lo que atañe a la protección de datos de carácter personal, el preámbulo de la norma resalta dentro de los principios particulares el de la protección de los datos de carácter personal.

En este sentido, la protección de datos de carácter personal se configura como primero de los principios particulares enumerados en el artículo 2.2 del Proyecto, indicando que “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”.

Dentro de la regulación de la estructura organizativa del departamento se determina que la misma estará compuesta, además de por el Comité de Dirección de Seguridad de la Información y el Grupo de Trabajo Técnico de Seguridad de la Información, por los Responsables de la Seguridad, los Responsables de la Información, Responsables del Servicio, Responsables del Sistema, así como por el Delegado de Protección de Datos.

Al regular la figura del Responsable de la Información, en el apartado 2 del artículo 7 señala que “A los efectos previstos en el Reglamento general de protección de datos, Reglamento (UE) 2016/679, los Responsables de la Información tendrán asimismo la consideración de responsables o encargados del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación. En particular, los Responsables de la Información deberán mantener los registros de las actividades de tratamiento a los que se refiere el artículo 30 del citado Reglamento. Dentro de las funciones de los Responsables de la Información, se encuentran las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información. Para ello, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

b) Colaborar, junto a los Responsables del Servicio, y contando con la participación del Responsable de la Seguridad, en la realización de los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

c) Son los responsables de aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos”.

En cuanto al Delegado de Protección de Datos, la única previsión específica es la contemplada en el artículo 5, que regula el Grupo de Trabajo Técnico de Seguridad de la Información (GTTS), al señalar en su apartado 5 que “El Delegado de Protección de Datos participará, con voz, pero sin voto, en las reuniones del GTTSI. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos”.

El artículo 13, lleva por rúbrica protección de datos de carácter personal, estableciendo que:

“Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Asuntos Económicos y Transformación Digital, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, tal cual se detalla en Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el Anexo II del Real Decreto 311/2022, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.”

II

El texto sometido a informe debe ser objeto de análisis atendiendo a lo dispuesto 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En efecto, como indica la Exposición de motivos de la Ley 3/2018 “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. De este modo, el cambio de aproximación de la normativa de protección de datos implica necesariamente una modificación en el enfoque que habrá de darse a las políticas de seguridad de la información, en que se evoluciona de un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos que deberá incardinarse en el texto ahora sometido a informe.

Así, el artículo 24.1 del Reglamento General de Protección de Datos dispone que “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual “Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados”.

A su vez, en relación con la seguridad de la información, el artículo 32.1 establece que “Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”.

Un papel fundamental, en fin, dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el Delegado de Protección de Datos, que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un Delegado en los supuestos en que “el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial”.

A su vez, el artículo 38.1 establece claramente que “El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales” y el artículo 39.2 dispone que “El delegado de protección de datos desempeñará sus funciones prestando la

debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento”.

Finalmente, el artículo 39.1 enumera las funciones del delegado de Protección de Datos, entre las que se encuentran “informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros” (apartado a), “supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes” (apartado b) y “ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).

III

De lo que acaba de indicarse se desprenden dos conclusiones que afectan sustancialmente al Proyecto objeto de informe: por una parte, la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone que las conclusiones del análisis de riesgos en materia de protección de datos y, en su caso, la evaluación de impacto en la misma, han de integrarse en la política de seguridad de la información, de modo que no se produzca una mera remisión a las normas de protección de datos, habida cuenta que éstas ya no establecen un modelo tasado de cumplimiento.

Por otra, el papel del Delegado de Protección de Datos, obligatorio en el supuesto que ahora se está analizando, resulta esencial en todo el diseño y desarrollo de la política de seguridad de la información, debiendo tener pleno conocimiento de la misma y asesorar en su diseño e implantación, en virtud de las funciones que el reglamento general de Protección de Datos le otorga expresamente.

No obstante, tal y como se indicó en el Informe 170/2018, de 12 de noviembre de 2018, relativo a la compatibilidad funcional del delegado de protección de datos del RGPD y el responsable de seguridad del Esquema Nacional de Seguridad, se hace preciso deslindar dichos ámbitos:

“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)”.

IV

Asimismo, debe destacarse que éste es el primer informe que se emite por esta Agencia respecto de una política de seguridad de la información tras la entrada en vigor del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el cual procedió a la actualización de dicha regulación para tener en cuenta, entre otros factores, la nueva

normativa sobre protección de datos personales, atendiendo a lo previsto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

En la nueva regulación de dicho Esquema se introdujeron los criterios mantenidos por la Agencia Española de Protección de Datos, en cuanto que la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento de los datos personales, quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de los interesados, pero sin que 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, a un conjunto de principios, derechos, medidas y garantías mucho más amplio, entre ellas medidas sobre el concepto del tratamiento, políticas de protección de datos, protección de datos desde el diseño y por defecto o notificación y comunicación de brechas de datos personales, bajo la garantía administrativa de las “autoridades de control” previstas en dicha normativa.

De este modo, el ENS incluirá medidas de seguridad que tienden a garantizar el cumplimiento de lo previsto en el artículo 32 del RGPD, pero sin que pueda entenderse de una manera excluyente y desvinculada del análisis de riesgos previsto en el artículo 24 del RGPD, subsistiendo la responsabilidad del responsable del tratamiento y, en su caso, de los encargados del tratamiento, de adoptar todas aquellas medidas adicionales a las contempladas en el ENS, en particular aquellas que van más allá de meras medidas de seguridad, que resulten necesarias para proteger los derechos y libertades de los afectados, teniendo en cuenta los criterios que, al respecto, se puedan

establecer por esta Agencia Española de Protección de Datos y, en su ámbito competencial, por las autoridades autonómicas de protección de datos personales.

Como consecuencia de lo anterior y para clarificar la relación existente entre la normativa sobre protección de datos personales y las medidas de seguridad del ENS, que solo serían una parte específica y limitada dirigida a garantizar su cumplimiento, pero que no excluye la aplicación del resto de dicha normativa, se introdujo la regulación contenida en el artículo 3 del Real Decreto 311/2022 (la negrita es nuestra):

Artículo 3. Sistemas de información que traten datos personales.

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto 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) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, **el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.**

3. En todo caso, **prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto** a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Y en su Anexo II, en el apartado 5.7.1 Datos personales [mp.info.1], que aplica a cualquier nivel de tratamiento, se establece:

– [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando

con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Consecuentemente, la política de seguridad de la información, en los sistemas que traten datos de carácter personal, vendrá predeterminada y condicionada por lo previsto en la normativa sobre protección de datos personales y las correspondientes políticas de protección de datos personales.

V

El Proyecto sometido a informe toma en cuenta estas consideraciones, si bien de manera limitada.

En este sentido, incluye al delegado de protección de datos dentro de la estructura organizativa de la gestión de la seguridad de la información, de modo que sea oído en todo caso en el diseño e implantación de dicha política de seguridad.

Asimismo, en su artículo 13, se ha tenido en cuenta el nuevo régimen de protección de datos, basado en la necesidad de realización del análisis de riesgos establecido en el artículo 24 del Reglamento y, en su caso, de la evaluación de impacto en la protección de datos a la que se refiere su artículo 35 para la determinación de las medidas que garanticen adecuadamente la seguridad de la información desde el enfoque de la protección de datos de carácter personal. Además, se recoge expresamente, tal y como ha venido informando esta Agencia, que las medidas a implantar como consecuencia del análisis de riesgos previsto en el artículo 24.1 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.

No obstante lo anterior, en la regulación proyectada se observa la falta de una visión conjunta e integrada de la gestión de riesgos en los sistemas de información que traten datos de carácter personal. De este modo, además de la gestión de riesgos de la seguridad, a la que se refieren el artículo 2.1.d) y el artículo 11, debe tomarse en consideración y con carácter previo la gestión de riesgos de la privacidad a la que se refiere el artículo 13, estableciendo la necesaria coordinación entre ambas atendiendo al resultado del análisis de

riesgos y, en su caso, de las evaluaciones de impacto relativas a la protección de datos.

De este modo, al referirse el artículo 2.1.d) al principio de gestión de riesgos y partiendo de que el análisis de riesgo específico para los derechos y libertades de los afectados, exigido por la normativa sobre protección de datos personales, va a sustentar y condicionar la política de seguridad y el análisis de riesgos regulado en su artículo 11, debe incluirse en el citado artículo 2.1.d) una referencia expresa a lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 3 del Real Decreto 311/2022, de 3 de mayo.

Asimismo, en el apartado 4 del artículo 11, al regular el proceso de evaluación del riesgo y de decisión del nivel de riesgo, debería incluir una referencia expresa a las previsiones del artículo 13, de modo que los requisitos identificados conforme al mismo y con el asesoramiento específico del DPD se puedan añadir a los establecidos conforme al ENS si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales son de alto riesgo, esos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por esta Agencia.

Por otro lado, se echa en falta una mención específica al artículo 32 del RGPD, el cual regula la seguridad del tratamiento:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Esta Agencia considera conveniente que en la Exposición de Motivos se recoja una referencia expresa a la normativa sobre protección de datos personales y, en particular al citado artículo 32 del RGPD y a la disposición adicional primera de la LOPDGDD.

Asimismo, en el artículo 13 debería incluirse la mención expresa del artículo 32 del RGPD, el cual exige una identificación de riesgos específicos para los derechos y libertades de las personas con relación a los tratamientos efectuados por la entidad, que debe ser previo al análisis de riesgos de los sistemas donde se implementen los tratamientos, tal y como ya se ha indicado, de modo que permita que el nivel de seguridad sea adecuado al riesgo que los tratamientos suponen para los derechos y libertades de las personas.

Por otro lado, debiendo garantizarse, en particular, la resiliencia en los tratamientos de datos personales, debería recogerse una referencia expresa al respecto en esta política.

Del mismo modo, la exigencia de “un proceso de verificación, evaluación y valoración regulares” implica la necesidad de incluir en la política que las auditorías a la que la misma hace referencia deberán ser regulares, definiendo la periodicidad correspondiente.

Por otro lado, y conforme a ese visión conjunta e integradora a la que se ha hecho referencia, siendo el responsable del tratamiento y, en su caso, el encargado, los obligados a dar cumplimiento a las previsiones de los artículos 24, 25 y 32 del RGPD, dentro del principio de responsabilidad diferenciada

recogido en el artículo 2.1.b) debería indicarse que “En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016”.

Y en el principio de seguridad por defecto y desde el diseño (artículo 2.1.g), teniendo en cuenta que la protección de datos personales es más amplia que la mera seguridad de los datos, debería añadirse una referencia expresa a la protección de datos personales, teniendo en cuenta que los artículos 24 y 25 prevén la adopción de medidas de seguridad por defecto, a diferencia del artículo 32 que se refiere a las medidas de seguridad orientadas al riesgo.

Por último, en cuanto a la letra h) del apartado 2 del mismo artículo 2, referido a la gestión de los incidentes de seguridad, debe completarse con la referencia a la aplicación de la normativa sobre protección de datos personales, tal y como prevé expresamente el apartado 4.3.7. del ENS:

- [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

A este respecto, debe tenerse en cuenta que los artículos 33 y 34 del RGPD establece tres obligaciones específicas: notificación, comunicación y documentación, orientadas a la obtención de resultados, lo que implica que la política debe implementar unos medios (organizativos y materiales) que garanticen que dichos resultados se va a obtener de forma eficaz, entre ellos, la implicación del DPD en dicha gestión de incidentes.

IV

Debe hacerse especial referencia, como ya se anticipó, a la figura del Delegado de Protección de Datos.

La inclusión del delegado de protección de datos dentro de la estructura organizativa vinculada con la seguridad de la información resulta, como se ha expuesto anteriormente, esencial dentro del esquema establecido en el Reglamento general de protección de datos. Y en ese sentido cabe valorar muy positivamente la referencia que el Proyecto hace de la citada figura.

Ahora bien, es necesario que dicha inclusión se lleve a cabo teniendo particularmente en cuenta cuál es la misión y las funciones del delegado de

protección de datos dentro del sistema de responsabilidad activa establecido por el mencionado Reglamento general.

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

En este sentido, el Reglamento es claro a la hora de imponer al responsable la obligación de cumplimiento de las medidas que el mismo prevé. Será así el responsable quien deberá mantener un registro de operaciones de tratamiento, evaluar el riesgo concurrente en un determinado tratamiento de datos o desarrollar en su caso a evaluación de impacto exigida por el reglamento. Del mismo modo, será el que 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 tuvieran atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos enumerados en los artículos 6 a 9 del Proyecto y, particularmente, el responsable de seguridad.

Frente a lo que acaba de indicarse, la función del delegado de protección de datos será 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”.

Por otro lado, en el citado Informe 170/2018 en relación con la diferenciación entre el DPD y el responsable de seguridad del ENS, se señalaba lo siguiente:

IV

Las posiciones del RSEG y del DPD son requisitos exigidos en normas diferenciadas con objetivos y ámbitos de aplicación distintos y, el principio de independencia del DPD, debería entenderse de manera amplia incluso con relación a las figuras que menciona el artículo 10 del ENS. En el mismo orden de ideas, cabría tener en cuenta que el propio principio de segregación de funciones del ENS tuviera en cuenta la separación de los roles indicados (RINF, RSEG, RSER) con relación a las funciones del DPD.

Debe de entenderse que la función de seguridad de la información es una herramienta que permite abordar el cumplimiento de lo previsto en el artículo 32 del RGPD, pero no puede entenderse como una herramienta que garantice el pleno e íntegro cumplimiento del RGPD. En consecuencia, las funciones del RSEG tienen un alcance limitado en el RGPD frente al alcance de las competencias del DPD.

Carece de sentido que se especifique la diferenciación de los tres roles relacionados con la seguridad de la información en las Administraciones Públicas, y se quiera asignar ahora un rol adicional, el de DPD, al responsable de seguridad de la información. Resulta claro que un DPD, alimentará de requisitos, aconsejará y supervisará a los tres responsables: información, servicio y seguridad. Si el responsable de seguridad asume las tareas de DPD, se le asigna de forma directa tareas de los otros dos responsables, lo que contradice el propio ENS y, sin duda, generaría posibles conflictos de intereses que podrían afectar a los derechos y libertades de las personas o incluso a la propia seguridad de la información.

En definitiva, esa diferenciación de tareas que garantiza la efectividad del trabajo del responsable de seguridad tiene sentido extenderla a que no se le asignen tareas no específicas de su función. Del mismo modo que la necesaria independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estará sujeto a instrucciones de otros órganos.

Así lo han entendido en organizaciones con importantes responsabilidades en materia de seguridad de la información. En este sentido, en el Ministerio de Defensa, en el que la información “constituye un recurso estratégico del Departamento sobre el que se debe buscar la superioridad para facilitar el cumplimiento y alcanzar el éxito de los cometidos encomendados al Ministerio de Defensa y de las misiones de las Fuerzas Armadas” (artículo 2 de la Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa), está dotado de una estructura que depende del Secretario de Estado de Defensa en cuanto órgano responsable de la

dirección, impulso y gestión de las políticas de las tecnologías, sistemas y seguridad de la información (artículo 4 del Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa) y que se desarrolla en diferentes órdenes ministeriales, además de la ya citada Orden DEF/1196/2017: la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa y la Orden ministerial 5/2017, de 9 de febrero por la que se aprueba la Política de Gestión de Documentos electrónicos del Ministerio de Defensa.

Sin embargo, el delegado de protección de datos ha sido designado al margen de dicha estructura, dependiendo directamente del Subsecretario de Defensa, con lo que se garantiza su independencia y se evita cualquier tipo de conflicto de intereses en el ejercicio de sus funciones.

V

En conclusión, es criterio de este Gabinete Jurídico que, con carácter general, debe existir la necesaria separación entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

Solo excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones

así como las medidas que garantizan la necesaria independencia del delegado de protección de datos.

El texto remitido respeta la separación de funciones anteriormente señalada, integrando al delegado de protección de datos en la estructura organizativa contemplada en el artículo 3 y diferenciando debidamente entre la figura del responsable de seguridad y la de delegado de protección de datos.

No obstante, la única mención que se contiene respecto del mismo es la contenida en el artículo 5.5 en cuanto participe en las reuniones del GTTSI.

Esta Agencia considera necesario que en la política se desarrolle aún más la intervención del delegado de protección de datos, al que podría dedicarse un artículo específico al igual que al resto de agentes que forman parte de dicha estructura, y en el que se recoja su implicación a lo largo del proceso de identificación y gestión de riesgos, incluido, como se ha señalado, su intervención en la gestión de las brechas de datos personales dentro de la gestión general de incidentes.

En todo caso, debe mantenerse su carácter asesor y supervisor, de modo que no le corresponde al mismo adoptar las decisiones oportunas, al ser esta función ejecutiva propia del responsable del tratamiento. Por ello se informa favorablemente que la participación del mismo en las reuniones del GTTSI lo sea con voz, pero sin voto, tal y como ha venido indicando esta Agencia.

Asimismo, debe recordarse lo manifestado por esta Agencia en el Informe 100/2019 respecto a la necesidad de dotar al DPD de los medios necesarios que permitan el adecuado ejercicio de sus funciones:

IV

Atendiendo a lo señalado en el presente informe, y ya al margen de lo solicitado en la presente consulta, esta Agencia debe incidir, una vez más, en la importancia que la figura del DPD tiene en el nuevo modelo instaurado por el RGPD y que pivota sobre la base de la responsabilidad proactiva del responsable. De acuerdo con el mismo, en los casos en que resulte obligatorio o así se haya estimado adecuado con carácter voluntario, ha de ser el responsable el que valore la procedencia de designar uno o varios DPD, así como si el mismo ha de pertenecer o no a su propia estructura, garantizando en todo momento su independencia y disponibilidad. Asimismo, deberá garantizar que el DPD cumple con los requisitos de capacitación adecuados y que se le dota de los medios personales y materiales necesarios para la realización eficaz de las funciones que tiene encomendadas, que participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales y que rinde

cuentas al más alto nivel jerárquico, documentando adecuadamente el responsable, conforme al ya citado principio de responsabilidad proactiva, todas las decisiones que adopte a este respecto, para poder demostrarlo a requerimiento de las autoridades de control. De este modo, quedará garantizado que el nombramiento del DPD no se ha realizado con carácter meramente formal y que el mismo cumple eficazmente con las funciones que le asigna el RGPD, siendo el primer interesado en dicha eficacia el propio responsable, que es quien responderá, y no el DPD, en caso de inobservancia del RGPD.

VI

A continuación, debe hacerse referencia a la regulación proyectada en el artículo 7 respecto de los responsables de la información, a los que se identifica con los responsables del tratamiento, lo que se pretende justificar en la MAIN señalando que “Si bien puede parecer un rol o tarea excesiva, estos responsables coinciden con los designados como responsables de tratamiento dentro del Reglamento General de Protección de Datos, que ya han sido nombrados (puede consultarse el Registro de Actividades de Tratamiento en la página web del Departamento)”.

Artículo 7. Responsables de la Información.

1. Los Responsables de la Información determinarán los requisitos sobre la información tratada y, por lo tanto, asumen la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

2. Los Responsables de la Información 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 Reglamento general de protección de datos, Reglamento (UE) 2016/679, los Responsables de la Información tendrán asimismo la consideración de responsables o encargados del tratamiento respecto de los datos personales contenidos en la información incluida en su ámbito de actuación. En particular, los Responsables de la Información deberán mantener los registros de las actividades de tratamiento a los que se refiere el artículo 30 del citado Reglamento. Dentro de las funciones de los Responsables de la Información, se encuentran las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información. Para ello, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

b) Colaborar, junto a los Responsables del Servicio, y contando con la participación del Responsable de la Seguridad, en la realización de los preceptivos análisis de riesgos y seleccionar las salvaguardas que se han de implantar.

c) Son los responsables de aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

3. Existirá un Responsable de la Información en cada órgano directivo, o superior en su caso, del Ministerio de Asuntos Económicos y Transformación Digital, así como en cada organismo o entidad de derecho público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI. Estos responsables se designarán de acuerdo con la organización interna del órgano respectivo, sin que, según lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

El Responsable de la Información se define en el artículo 13.2.a) del Real Decreto 311/2022, de 3 de mayo, al señalar que “El responsable de la información determinará los requisitos de la información tratada”, refiriéndose a los requisitos de seguridad de la misma. Por su parte, el concepto de responsable del tratamiento se recoge en el artículo 4. 7) del RGPD: «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”. Por consiguiente, el responsable de la información únicamente podrá tener la consideración de responsable del tratamiento en la medida en que sea el que determine, solo o junto con otros, los fines y medios del tratamiento, lo que deberá analizarse caso por caso y atendiendo al nivel de responsabilidad y capacidad de decisión correspondiente.

Por tanto, debe suprimirse dicha identificación de responsabilidades.

VII

Por último, debe hacerse referencia a los tratamientos de datos personales que puedan realizarse como consecuencia de la implantación de medidas de seguridad que tengan un objetivo distinto que la protección de datos personales, cuestión que fue igualmente objeto de análisis en nuestro informe 64/2021, sobre el Proyecto de Real Decreto por el que se regula el Esquema Nacional de Seguridad, y cuyas observaciones han sido incorporadas al Real Decreto 311/2022, de 3 de mayo:

III

Para concluir, además de las observaciones sustanciales recogidas en el apartado anterior debe resaltarse que, al igual que las medidas de seguridad aplicables a los sistemas de información que traten datos personales deben adecuarse a la normativa sobre protección de datos personales, al objeto de dotarlos de una protección ajustada a la misma, dicha normativa deberá aplicarse igualmente a aquellas medidas de seguridad previstas en el ENS que, independientemente de los sistemas a los que se apliquen, supongan tratamientos de datos personales, lo que requerirá, entre otros requisitos, una adecuada valoración de la proporcionalidad de las mismas.

Así se recoge, por ejemplo, en el artículo Artículo 24, que regula el Registro de la actividad y detección de código dañino:

Con el solo propósito de satisfacer el objeto del presente 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, se registrarán las actividades de los usuarios, reteniendo la información 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 (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), los sujetos comprendidos en el artículo 2 de este real decreto podrán analizar las comunicaciones entrantes o salientes, 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.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe

derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Aun cuando en este supuesto, al referirse a tratamientos de datos personales vinculados a la actividad de las Administraciones Públicas, la base jurídica que legitima dichos tratamientos se encontraría en la letra e) del artículo 6.1 del RGPD “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”, al no ser aplicable a los tratamientos de la Administración el interés legítimo, tal y como se señaló en nuestro Informe 175/2018, procede traer a colación lo señalado en el Considerando 49 del RGPD, en cuanto se refiere específicamente a la “seguridad de la red y de la información”:

Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

*De dicho Considerando interesa destacar la importancia que se da a que el tratamiento lo sea **“en la medida estrictamente necesaria y proporcionada”**, ya que siendo los principios de necesidad y de proporcionalidad principios aplicables a todos los tratamientos de datos personales conforme al artículo 5.1. del RGPD, el propio legislador comunitario ha querido destacar específicamente en este supuesto.*

Del mismo modo, dicho principio de proporcionalidad ha sido reiteradamente destacado por nuestro Tribunal Constitucional, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo, F. 5; 55/1996, de 28 de marzo, FF. 7, 8 y 9; 270/1996, de 16 de diciembre, F. 4.e; 37/1998, de 17 de febrero, F. 8; 186/2000, de 10 de julio, F. 6).”

Por ello, debería recogerse en el texto del citado artículo 24 una referencia expresa a los citados principios, proponiéndose la siguiente redacción:

Registro de la actividad y detección de código dañino:

*Con el solo propósito de satisfacer el objeto del presente 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, se registrarán 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 (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), los sujetos comprendidos en el artículo 2 de este real decreto podrán, **en la medida estrictamente necesaria y proporcionada**, analizar las comunicaciones entrantes o salientes, 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.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

*Por otro lado, siendo la presente norma la que establece los correspondientes tratamientos de datos personales, **debería incluirse en dicho precepto o en los Anexos otras garantías adicionales concretas, derivadas de los demás principios del artículo 5 del RGPD**, como pueden ser, entre otros, el principio de limitación de la finalidad, prohibiendo el tratamiento de los datos personales para fines distintos; del principio de minimización de datos, identificando los datos personales o las categorías de datos personales que pudieran ser tratados; o del principio de limitación del plazo de conservación, identificando los plazos máximos de conservación de los datos personales.*

Estas cautelas deben ser especialmente rigurosas en lo que se refiere al análisis de las comunicaciones entrantes y salientes al que hace referencia el segundo párrafo del precepto, para evitar que se vulneren los derechos fundamentales de los afectados, incluido, además del de la protección de datos personales, el del secreto de las comunicaciones, cuya limitación requeriría norma con rango de ley ajustada a los principios señalados por la jurisprudencia del Tribunal Constitucional.

Tal y como resulta del citado informe, si la implementación de medidas de seguridad con otras finalidades (por ejemplo, continuidad de procesos, seguridad física, seguridad del Estado, protección de la confidencialidad de la información, la propiedad intelectual o la industrial, etc.) supone un tratamiento adicional de datos personales deberá procederse al cumplimiento íntegro del RGPD y, en particular y como señala el propio Considerando 49, realizar un análisis de si el tratamiento es una medida “estrictamente necesaria y proporcionada”, para cuya valoración deberá contarse con el asesoramiento del DPD.

De esta forma, se considera necesario especificar que las labores de asesoramiento y supervisión del DPD en cuanto a las políticas de seguridad no se han de limitar a supervisar la implementación de medidas para garantizar la protección de datos, sino también aquellas otras medidas que se pretenda

implantar con el propósito de garantizar otros objetivos y que impliquen un tratamiento adicional de datos personales.

Por ello, al regular la intervención del DPD debería añadirse una referencia al asesoramiento y la supervisión por parte del DPD de medidas de seguridad que tengan un objetivo distinto que la protección de datos, en la medida en que impliquen un tratamiento adicional de datos personales.