

N/REF: 0064/2021

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Proyecto de Real Decreto por el que se regula el Esquema Nacional de Seguridad, solicitado de esta Agencia Española de Protección de Datos (AEPD) de conformidad con lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en relación con el artículo 57.1, letra c), del 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 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 389/2021, de 1 de junio, cúpleme informarle lo siguiente:

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.

El proyecto remitido tiene por objeto regula el Esquema Nacional de Seguridad, establecido en el apartado 2 del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, para asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, informaciones y servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

De este modo, se procede a una actualización del Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010, de 8 de enero, para adecuarlo a los notables cambios acaecidos tras su actualización en 2015 y que destaca su preámbulo: la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad o el avance de las tecnologías de aplicación. Todo ello, con modificaciones del marco legal en materia de procedimiento administrativo y régimen jurídico del sector público, seguridad de las redes y sistemas de información, así como el de protección de datos y del marco estratégico de ciberseguridad, con la Estrategia de 2019. Además, se ha extendido la implantación del ENS con una mayor experiencia acumulada

sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por el CCN-CERT, del Centro Criptológico Nacional (CCN).

Dicha actualización se realiza atendiendo a tres grandes cuestiones: alinear el ENS con el marco normativo y el contexto estratégico existente para facilitar la seguridad en la Administración Digital, introducir la capacidad de ajustar los requisitos del ENS para adaptarse a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y servicios y facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua.

En relación con la protección de datos de carácter personal, el preámbulo de la norma hace referencia tanto a 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 y al artículo 37 de 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, señalando lo siguiente:

A lo anterior se añadió 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 que establece que el ENS incluirá aquellas medidas que deberán 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, 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 que prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público e, indirectamente, a las del Sector Privado que colaboren con aquellas en la prestación de servicios públicos que involucren el tratamiento de datos personales. En este mismo sentido, el artículo 37 de 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, establece la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

En cuanto al articulado, y respecto de los sistemas de información que traten datos de carácter personal, contiene únicamente dos previsiones:

Por un lado, el artículo 28, referido a los requisitos mínimos, señala en su apartado 2 lo siguiente:

“2. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en especial su Disposición adicional primera 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, en especial su artículo 37, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el presente real decreto.”

Y la disposición adicional cuarta, referida a la aplicación de los requisitos del Esquema Nacional de Seguridad a los sistemas de información que permitan los tratamientos de datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y con 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, añade lo siguiente:

En aplicación de lo dispuesto en el artículo 28.2 de este real decreto, los requisitos establecidos en el mismo se aplicarán a los sistemas de información que permitan los tratamientos de datos personales en el ámbito subjetivo y con el alcance al que se refieren el artículo 77.1 y la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, o en su caso, el artículo 2 y artículo 37 de la Ley Orgánica 7/2021, de 26 de mayo.

En el Anexo II, referido a las Medidas de Seguridad, se refiere a los datos personales en su apartado 5.7.1., remitiendo a la aplicación de su normativa específica y estableciendo como refuerzo R1 la anonimización y seudonimización de datos personales y como refuerzo R2 el tratamiento con fines estadísticos.

Con carácter previo al análisis del texto remitido, y para enmarcar adecuadamente la relaciones existentes entre la seguridad de la información y la protección de datos de carácter personal, esta Agencia considera necesario poner de manifiesto, una vez más, las diferencias existentes entre dichos ámbitos, y en las que ha venido incidiendo desde la plena aplicación del RGPD en los distintos informes que se le han solicitado.

En este sentido, incluso con anterioridad a la aprobación de la LOPDGDD, el Informe 170/2018, en el que se apreciaba, con carácter general, la incompatibilidad entre la figura del delegado de protección de datos del Reglamento general de protección de datos y el responsable de seguridad de la información del Esquema Nacional de Seguridad, se señalaba lo siguiente:

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).

Asimismo, en los sucesivos informes emitidos sobre las políticas de seguridad de la información de los diferentes departamentos ministeriales, esta Agencia viene recalcando cómo la nueva normativa sobre protección de datos personales ha supuesto una evolución desde un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos en el que asume una importante labor la nueva figura del delegado de protección de datos. En este sentido, procede traer a colación lo indicado en nuestro Informe 52/2019:

“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).

Y como consecuencia de dicho cambio normativo, se extraen las siguientes consecuencias, que se reiteran en el último informe emitido al respecto, el Informe 57/2021:

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 el análisis de riesgos en materia de protección de datos y, en su caso la evaluación de impacto en la misma, pase a formar parte integrante de 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.

Y teniendo en cuenta lo anterior, el citado informe 57/2021 destacaba cómo la política de seguridad de la información analizada se ajustaba a las exigencias de la normativa sobre protección de datos personales:

El Proyecto sometido a informe toma en cuenta estas consideraciones, por cuanto incluye al delegado de protección de datos dentro de la

estructura organizativa de la gestión de la seguridad de la información y atribuyendo al mismo las funciones que establece el propio Reglamento, de modo que sea oído en todo caso en el diseño e implantación de dicha política de seguridad.

Asimismo, partiendo de una visión conjunta de la gestión de riesgos en el artículo 4.1.d), se diferencia por un lado la gestión de riesgos de la seguridad, a la que se refiere el artículo 15, y la gestión de riesgos de la privacidad a la que se refiere el artículo 16, estableciendo la necesaria coordinación entre ambas atendiendo al resultado del análisis de riesgos y, en su caso, de la evaluaciones de impacto relativas a la protección de datos. Por tanto, 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.

Por último, conviene hacer referencia, igualmente, al Informe 122/2019, referente al Proyecto de Real Decreto por el que se desarrolla el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en el que se incluyeron diversas observaciones sustanciales. La primera, en cuanto a las medidas para el cumplimiento de las obligaciones de seguridad que deberán adoptar los operadores de servicios esenciales y los proveedores de servicios digitales, respecto de las que el texto contenía una remisión al ENS, la necesidad de tener en cuenta los riesgos que se derivan del tratamiento de los datos personales de acuerdo con el artículo 24 del RGPD, y que “debería clarificarse 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 deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos”. La segunda, que la compatibilidad que se reconocía entre la figura del “Responsable de la seguridad de la información” y la del DPD era contraria al RGPD, conforme al criterio reiterado de esta Agencia. Y la tercera, referida a la gestión de incidentes de seguridad, respecto de la necesidad de cumplir “en todo caso, siempre que se produzca una violación de la seguridad de los datos personales, con la obligación de notificación a la autoridad de control de protección de datos competente, en los términos previstos en el artículo 33 del

RGPD, y sin perjuicio de la cooperación entre autoridades prevista en el artículo 29 del Real Decreto Ley 12/2018, y la posibilidad de acceso por parte de la AEPD a la plataforma común de notificación de incidentes prevista en su disposición adicional tercera”.

II

Partiendo de lo anterior, esta Agencia considera que las referencias que el proyecto remitido contiene a la normativa sobre protección de datos personales son insuficientes para garantizar un adecuado cumplimiento de la misma, en la que, como se ha indicado, 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 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.

Dentro de este concepto amplio de protección de datos personales debe encuadrarse la disposición adicional primera de la LOPDGDD:

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.

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.

En este punto, es relevante destacar que el proyecto remitido se centra en los sistemas de información, y no en los tratamientos de datos personales, así como en los riesgos que pueden afectar a la seguridad de los mismos, pero no en los riesgos que puedan implicar los tratamientos para los derechos y libertades de los afectados, que es el eje central de toda la normativa sobre protección de datos personales, por lo que la regulación contenida en el mismo es insuficiente para garantizar una adecuada protección del derecho fundamental.

Por todo ello, 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 considera imprescindible** que se incluya en las disposiciones generales, a continuación del ámbito de aplicación, **un artículo específico** en el que así se determine, con la siguiente redacción:

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 General de Protección de Datos y 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 consecuentemente, deberá suprimirse el apartado 2 del artículo 28 y la disposición adicional cuarta al resultar innecesaria.

Por las mismas razones expuestas, **debe modificarse el apartado 5.7.1. del Anexo II**, para adecuarse a los requisitos exigidos por la normativa sobre protección de datos personales:

5.7.1. Datos personales [mp.info.1] Requisitos

[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.

Asimismo, **debe eliminarse la referencia a los refuerzos R1 y R2**, ya que dichos refuerzos vendrán determinados en cada caso por el análisis de riesgos y, en su caso, por la evaluación de impacto.

Por otro lado, para garantizar que la normativa sobre protección de datos personales y, en particular, el análisis de riesgos en materia de protección de datos y, en su caso la evaluación de impacto en la misma, pasa a formar parte integrante de la política de seguridad de la información, **debe incluirse una nueva letra en el artículo 12.1**, de modo que en el contenido mínimo del instrumento que apruebe la política de seguridad incluya **los riesgos que se derivan del tratamiento de los datos personales**,

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.