

I

La norma que se informa responde a la previsión del artículo 12.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, RD 311/2022 o el ENS), que exige que en la Administración General del Estado cada ministerio cuente con su política de seguridad que aprobará la persona titular del Departamento.

El proyecto obedece al objetivo de actualizar la vigente política de seguridad del Ministerio de Trabajo y Economía Social (MTES) para adecuarla al marco jurídico actual, a la administración electrónica y a la evolución tecnológica. Por consiguiente, el proyecto prevé (disposición derogatoria única) la derogación de la Orden TES/369/2023, de 10 de abril, por la que se aprobó la actual política de seguridad.

A ese respecto, el Preámbulo del proyecto y la Memoria de Análisis de Impacto Normativo (MAIN) que le acompaña explican que *“la evolución normativa y tecnológica, las nuevas exigencias derivadas del Esquema Nacional de Seguridad, la incorporación de la vigilancia continua y la gestión dinámica del riesgo, así como la sucesiva reestructuración ministerial dada por los Reales Decretos 829/2023, 1009/2023 y 502/2024, hacen necesaria la actualización integral de dicho marco”*.

El Preámbulo del proyecto destaca también la incorporación de *“nuevos principios como el de mínimo privilegio, la clasificación de la información, la protección del soporte no electrónico y la vigilancia continua de los sistemas.”*

La norma se estructura en un preámbulo y una parte dispositiva, esta última integrada por dieciocho artículos, una disposición adicional, una derogatoria, dos disposiciones finales y un Anexo.

Constituye su objeto (**artículo 1**) la *aprobación* de la Política de Seguridad de la Información (en adelante, Política de Seguridad o PSI) y de los Servicios en el ámbito de la Administración Digital del MTES, la *redefinición* del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del MTES y la *regulación* de su composición, funcionamiento y funciones.

El ámbito de aplicación material y subjetivo del proyecto se regula en el **artículo 2**:

(I) En cuanto al ámbito material, la PSI se aplicará *“a todos los sistemas de información”*. La PSI comprende las orientaciones o directrices que rigen en el MTES la actuación de las personas y entidades en relación con la seguridad de los sistemas de información. El precepto ofrece un concepto legal de *“Sistema de Información”*, que define como *“un conjunto organizado de recursos (físicos, lógicos, de comunicación, de datos, procedimientos, de servicios contratados y personas) que permite conseguir las especificaciones funcionales establecidas para el departamento.”*

(II) En cuanto al ámbito subjetivo de aplicación, la PSI del MTES se aplicará a las actuaciones de las *“personas y entidades”* y previene que será de cumplimiento obligado para:

(i.) todo el personal que desempeñe sus funciones en el MTES y que acceda a los sistemas de información y a la información del departamento, con independencia de su adscripción profesional (empleados públicos y apoyo técnico de empresas)

(ii.) *“los órganos superiores y directivos del Ministerio”* y

(iii.) *“sus organismos públicos adscritos, que no tengan establecida su propia política de seguridad”*.

Esa última previsión, relativa al sector público institucional vinculado al MTES, es acorde con lo dispuesto en el RD 311/2022, cuyo artículo 12.2 determina que cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente, si bien añade a continuación que *“No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.”*

Adicionalmente, el artículo 2 del proyecto resuelve las discrepancias que puedan surgir entre la PSI que algunos órganos y organismos públicos vinculados al MTES puedan tener definida y la contemplada en la orden proyectada, disponiendo que prevalecerá esta última.

El artículo 12 del ENS, apartado 6, dispone que la PSI *“se establecerá de acuerdo con los principios básicos de seguridad de la información recogidos en el capítulo II”* –principios que conforme al artículo 5 del ENS son la seguridad como proceso integral, la gestión de la seguridad basada en los riesgos, la prevención, detección, respuesta y conservación, la existencia de líneas de defensa, la vigilancia continua: la reevaluación periódica y la diferenciación de responsabilidades– y se desarrollará “aplicando los

siguientes requisitos mínimos”: Organización e implantación del proceso de seguridad. Análisis y gestión de los riesgos. Gestión de personal. Profesionalidad. Autorización y control de los accesos. Protección de las instalaciones. Adquisición de productos de seguridad y contratación de servicios de seguridad. Mínimo privilegio. Integridad y actualización del sistema. Protección de la información almacenada y en tránsito. Prevención ante otros sistemas de información interconectados. Registro de la actividad y detección de código dañino. Incidentes de seguridad. Continuidad de la actividad y mejora continua del proceso de seguridad.

Pues bien, el proyecto que se informa da cumplimiento a lo dispuesto en el artículo 12.6 del ENS. Así, de una parte, su **artículo 4.2** incorpora los *principios básicos* de la seguridad de la información que establece el artículo 5 del ENS. De otra, el **artículo 5** establece los requisitos mínimos de seguridad de acuerdo con la relación que de ellos hace el artículo 12.6 del ENS.

En lo que atañe a la “*estructura organizativa*” a la que el MTES encomienda “*la gestión de la seguridad de sus sistemas de información*”, el proyecto dedica a su regulación los **artículos 6 a 14** estableciendo el **artículo 6** que está integrada por los siguientes sujetos:

(i) el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones –COSTIC— (artículos 7 a 9); (ii) las personas *responsables de los sistemas de información* (artículo 10); (iii) las personas *responsables de la información* (artículo 11); (iv) las personas *responsables de los servicios* (artículo 12); (v) las personas *responsables de la seguridad* (artículo 13); (vi) la persona *designada como Delegado/a de Protección de Datos*; (vii) las personas *responsables del tratamiento de datos personales*; (viii) las personas *encargadas del tratamiento de datos personales*; (ix) las personas *responsables de la prestación de los servicios TIC*.

II

Centrando el análisis del proyecto en su adecuación a la normativa de protección de datos de carácter personal, es obligado citar el artículo 3 del ENS:

“1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 [...] (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, [...], 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.

La disposición transcrita remite, para el caso de que un sistema de información trate datos personales, a la normativa de protección de datos de carácter personal y no exclusivamente a la obligación prevista en el artículo 32 del RGPD de adoptar medidas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Como explica el Informe 85/2022 del Servicio Jurídico de la AEPD, la seguridad de la información es una obligación más entre las que la normativa de protección de datos impone a los responsables y encargados de 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.”

Del citado Informe 85/2022 resulta que las medidas de seguridad que se adopten en aplicación del RD 311/2022 estarán encaminadas a garantizar el cumplimiento de lo dispuesto en el artículo 32 del RGPD, si bien tales medidas no podrán en ningún caso entenderse desvinculadas del análisis de riesgos previsto en el artículo 24 del RGPD y subsistirá siempre la responsabilidad del responsable del tratamiento (y en su caso del encargado) de adoptar medidas técnicas y organizativas “adicionales a las contempladas en el ENS” que resulten necesarias para garantizar una protección adecuada al nivel del riesgo que entrañe el tratamiento para los derechos y libertades de los interesados.

En esa línea argumental, el Informe 85/2022 afirma: “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.

El Preámbulo de la LOPDGDD señala , y así se recoge reiteradamente en los informes del Servicio Jurídico de esta AEPD, que el RGPD representa la evolución de un modelo basado en el control del cumplimiento a otro que descansa en el principio de responsabilidad proactiva.

En tal sentido, el artículo 5.2 del RGPD introduce el principio de responsabilidad proactiva en virtud del cual el responsable del tratamiento será responsable de cumplir los principios que presiden el tratamiento de datos establecidos en el artículo 5.1 y de poder demostrar su cumplimiento, debiendo adoptar a tal fin medidas técnicas y organizativas apropiadas en función de diversos factores, entre ellos los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas que entrañe el tratamiento (ex artículo 24). Las medidas apropiadas estarán concebidas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados (ex artículo 25). El RGPD obliga al responsable, y también al encargado de tratamiento, a aplicar las medidas apropiadas, técnicas y organizativas, para garantizar un nivel de seguridad adecuado al riesgo (ex artículo 32). Y, asimismo, obliga al responsable, en determinados supuestos, antes del tratamiento, a evaluar el impacto en la protección de datos personales de la operación de tratamiento que prevé realizar cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de la persona, en particular si utiliza nuevas tecnologías (ex artículo 35).

Por ello, los preceptos del RGPD exigen que el responsable del tratamiento lleve a cabo una *previa valoración del riesgo* que para los derechos y libertades de las personas físicas podría entrañar el tratamiento de datos que se prevé realizar. Le imponen la obligación de adoptar –teniendo en cuenta, entre otros elementos, el resultado de esa valoración– las medidas técnicas y organizativas que procedan conforme a los artículos 24 (medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento) y 32 del RGPD (medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo).

A ese respecto, el Informe del Servicio Jurídico 103/2022 (epígrafe III), tomando en consideración el nuevo modelo de cumplimiento, basado en la responsabilidad activa, que representa el RGPD, a la luz de sus artículos 24.1 y 32.1 y del considerando 75, afirma 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.

Partiendo de las consideraciones precedentes, cabe destacar del proyecto que se informa que prevé el pleno sometimiento de los tratamientos de datos que se efectúen en su ámbito aplicación a la normativa reguladora del derecho fundamental a la protección de datos de carácter personal:

El **artículo 3**, “*Marco normativo*”, dispone que las actividades del MTES en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las disposiciones contenidas en el anexo, así como sus actualizaciones normativas, y el citado anexo relaciona en primer lugar (letras a. y b. respectivamente) el RGPD y la LOPDGDD.

Además, son varios los preceptos del proyecto que remiten específicamente a la normativa reguladora de este derecho fundamental. Puede mencionarse el artículo 4, “*Principios de la Política de Seguridad*”, apartado 2 letras a), d) y h); el artículo 5, “*Requisitos de seguridad de la información*”, apartados b, (*Análisis y gestión de riesgos*), h (“*Mínimo privilegio*) y o (*Gestión de incidentes*); el artículo 14, “*Delegado o delegada de protección de datos*”; el artículo 15, “*Tratamiento de datos personales*” y el artículo 17, “*Actuación y efectos respecto a la información correspondiente a otros entes o servicios de competencia ajena al departamento*”, apartado 4.

Por otra parte, el **artículo 4** del proyecto, “***Principios de la Política de Seguridad***”, es un exponente de que la norma que se informa **se adecúa al RGPD y evidencia el propósito del proyecto de integrar en la política de seguridad del MTES las exigencias inherentes a la normativa de protección de datos.**

El **artículo 4** de la orden sigue en lo esencial la regulación que sobre los principios básicos de seguridad contiene el RD 311/2022, capítulo II, artículos 5 a 11. El ENS relaciona en su artículo 5, apartados a) a g), los “*Principios básicos del Esquema Nacional de Seguridad*” y los desarrolla en los artículos siguientes, dedicando en particular los artículos 6 y 7, respectivamente, a “*La seguridad como proceso integral*” y a la “*Gestión de la seguridad basada en los riesgos*”.

El **artículo 4** del proyecto comienza señalando (**apartado 1 y primer inciso de su apartado 2**), que la PSI del MTES aplicará los principios básicos que se establecen en el ENS “*permitiendo una protección adecuada de la información y de los servicios*”, de acuerdo con el interés general, la naturaleza y la complejidad de la materia regulada. A continuación, dispone que las medidas de seguridad, que serán *proporcionadas* a la naturaleza de la

información y de los servicios a proteger, se implementarán bajo los principios que relaciona en los apartados a) a h):

“a) Protección de datos personales. 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 datos de carácter personal.

b) Alcance estratégico. [...].

c) Seguridad Integral. [...]

d) Análisis y gestión de riesgos: todos los sistemas afectados por la PSI, así como todos los tratamientos de datos personales, serán objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis, que deberá ajustarse, en todo caso, a un criterio de proporcionalidad a los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados, y de acuerdo con los artículos 24, 25 y 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), así como el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales y el artículo 3 del RD 311/2022, cuando el sistema de información trate datos personales, se realizará:

1.º Regularmente, al menos una vez al año, revisando la situación del Sistema de Información para determinar si se han producido cambios que requieran una actualización en materia de seguridad.

2.º Cuando cambie la información manejada o los servicios prestados de manera significativa.

3.º Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

e) Prevención, reacción, recuperación y respuesta. [...]

f) Líneas de defensa. [...]

g) Vigilancia continua y reevaluación periódica. [...]

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección.

h) Función diferenciada: [...]

En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado 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.”

Pues bien, la letra **a) del artículo 4.2**, bajo la rúbrica “Protección de datos personales”, incorpora a la PSI del MTES la obligación que el artículo 32

del RGPD (*“Seguridad del tratamiento”*) impone al responsable y al encargado del tratamiento de aplicar *“medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”*.

En lo relativo al *nivel de seguridad* de las medidas, el artículo **4.2.a)** del proyecto dice que estarán destinadas a garantizar el *“exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal”*; referencia que debe entenderse como una remisión al texto del artículo 32 del RGPD que prevé que las medidas técnicas y organizativas se adopten 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.”*

Sobre este particular, el **artículo 15** del proyecto, *“Tratamiento de datos personales”*, dispone en su **apartado 1** que *“Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Trabajo y Economía Social las medidas de seguridad apropiadas derivadas del análisis de riesgos de privacidad, así como de la evaluación de impacto relativa a la protección de datos, tal y como se detalla en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.”*

En cuanto a la previsión de la letra **d)**, *“Análisis y gestión de riesgos”*, del **artículo 4.2.** del proyecto, obliga a que sean objeto de un análisis de riesgos *“todos los tratamientos de datos personales”* que se efectúen en su marco de aplicación y, además, *“todos los sistemas afectados por la PSI”* del MTES.

A tenor de este precepto (letra **d**, del **artículo 4.2**) el **objeto del análisis de riesgos** es *“evaluar las amenazas y los riesgos a los están expuestos”* tanto los tratamientos de datos como los sistemas de información del MTES incluidos en el ámbito de esta PSI. El proyecto exige que el análisis de riesgos se ajuste “en todo caso, a un criterio de proporcionalidad a los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados”.

Tal previsión está en consonancia con el artículo 7.2 del ENS, que, al regular la gestión de la seguridad basada en los riesgos, dispone que se minimizarán a niveles aceptables y añade que *“La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.”*

Debe subrayarse que, tanto el **artículo 4.2.d)** como el **artículo 15** del proyecto, **contienen reglas sobre el análisis de riesgos** que son de **aplicación exclusiva a los tratamientos de datos de carácter personal** que se efectúen en los sistemas de información incluidos en su ámbito de aplicación:

-El artículo **15.1, párrafo tercero**, del proyecto establece que *“La identificación de los riesgos específicos para los derechos y libertades de las personas físicas en relación con los tratamientos efectuados por la entidad debe ser previo al análisis de riesgos de sistemas donde se implementen los tratamientos, con el fin de permitir que el sistema de seguridad sea adecuado al riesgo que los tratamientos suponen para los derechos y libertades de las personas.”*

-El artículo **15.1, párrafo segundo**, del proyecto, informa (de acuerdo con la normativa de protección de datos) de a quién corresponde efectuar el análisis de riesgos cuando el sistema trate datos de carácter personal: *“la persona responsable o la persona encargada del tratamiento, asesoradas por la persona designada como delegada de protección de datos, realizarán un análisis de riesgos, conforme al artículo 24 del”* RGPD.

-El artículo **4.2.d)**, para el caso de que un sistema de información trate datos personales, incluye criterios temporales para llevar a cabo el análisis de riesgos. Cabe recordar que también existen criterios de esa naturaleza en los preceptos del RGPD a los que se hace mención en esta disposición del proyecto:

Así, el artículo 24.1 del RGPD (que obliga al responsable del tratamiento a adoptar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD) dice expresamente *“que se revisarán y actualizarán cuando sea necesario.”* El artículo 25 del RGPD alude al *“momento de determinar los medios de tratamiento”* y al *“momento del propio tratamiento”* como referencias temporales en las que el responsable tiene la obligación de adoptar las medidas técnicas y organizativas apropiadas concebidas para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento. Y el artículo 32.2 del RGPD dispone que *“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.”*

El **artículo 4.2.d)** del proyecto prevé que el análisis de riesgos se realice *regularmente, al menos una vez al año, a fin de determinar si se han producido cambios que requieran una actualización en materia de seguridad.* También cuando cambie la información manejada o los servicios prestados de manera significativa. Y cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

La previsión del **artículo 4.2.d)** del proyecto es plenamente acorde con la normativa de protección de datos que obliga al responsable a garantizar el

cumplimiento de los principios que presiden el tratamiento de los datos durante todo el ciclo de vida del tratamiento. Resultan esclarecedores sobre tal cuestión los epígrafes 37 y 38 de las Directrices 4/2019 del Comité Europeo de Protección de Datos (CEPD), relativas al artículo 25, Protección de datos desde el diseño y por defecto, Versión 2.0, adoptadas el 20 de octubre de 2020, que pasamos a reproducir:

“37. Una vez iniciado el tratamiento, el responsable tiene la obligación permanente de mantener la PDDD, es decir, aplicar los principios de forma efectiva y continuada a fin de proteger los derechos, mantenerse al día del estado de la técnica, reevaluar el nivel de riesgo, etcétera. La naturaleza, el ámbito y el contexto de las operaciones de tratamiento, así como el riesgo, pueden cambiar durante el curso del tratamiento, lo que significa que el responsable deberá reevaluar sus operaciones de tratamiento revisando y valorando periódicamente la efectividad de las medidas y garantías que haya decidido adoptar.”

“39. Esta obligación también se extiende a todo tratamiento realizado a través de encargados. Los responsables del tratamiento deben revisar y evaluar periódicamente las operaciones de los encargados del tratamiento para asegurarse de que hacen posible el cumplimiento continuo de los principios y permiten al responsable cumplir con sus obligaciones a este respecto.”

Finalmente, a propósito de la disposición del **segundo párrafo** de la letra **h) del artículo 4.2** del proyecto –que exige, cuando los sistemas traten datos personales, que la PSI identifique a “la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con el artículo 4, apartados 7 y 8” del RGPD–, basta añadir que, conforme a lo dispuesto en el artículo 30 del RGPD, en conexión con el artículo 31. 2 de la LOPDGDD, el inventario de actividades de tratamiento que la Administración General del Estado tiene la obligación de publicar por medios electrónicos incluirá, entre otra información, *el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos*.

En atención a lo expuesto, se **informa favorablemente el contenido del artículo 4 del proyecto objeto de análisis (principios de la política de seguridad), cuya regulación es coherente con la normativa de protección de datos de carácter personal**.

III

Entre los *requisitos mínimos de seguridad* que debe incluir toda PSI, el artículo 12.6 del ENS menciona en la letra b) el “*Análisis y gestión de los riesgos*”.

El **artículo 5** del proyecto, “*Requisitos de la seguridad de la información*”, dedica el apartado **b)** al “*Análisis y gestión de los riesgos*” y concibe la gestión del riesgo como un *proceso* consistente en la “*identificación, análisis, evaluación y tratamiento a los que el sistema esté expuesto.*” Indica que las medidas adoptadas para mitigar o suprimir los riesgos “*deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos*”, reproduciendo así, parcialmente, el texto del artículo 14 del ENS.

El **artículo 5.b)** contiene normas específicas sobre el análisis y la gestión de los riesgos para el caso de que el tratamiento afecte a datos de carácter personal. Así, su **párrafo segundo** previene que cuando un sistema de información trate datos personales, el responsable o el encargado, asesorado por el delegado de protección de datos, realizará un análisis de riesgos conforme al artículo 24 del Reglamento [...] y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.”

Por lo que atañe al **último párrafo del artículo 5.b)**, nos remitimos a las consideraciones que se hacen en el epígrafe siguiente.

El **artículo 5.b)**, **párrafo segundo**, debe conectarse con el **artículo 15.1**, “*Tratamiento de datos personales*”, a tenor del cual, para el caso de que un sistema de información trate datos personales, el análisis de riesgos se efectuará conforme al artículo 24 del RGPD (párrafo segundo del precepto) y las medidas de seguridad que se adopten serán las apropiadas según detalla el artículo 32 del RGPD (párrafo primero del precepto).

Añade el **artículo 15.1** (párrafo **cuarto**) que cuando “*sea probable que un tipo de tratamiento [...] entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con lo establecido en el artículo 35*” del RGPD.

Por otra parte, en relación con las medidas que deben adoptarse, el **artículo 5** del proyecto, letra **h)**, “*Mínimo privilegio*”, se remite expresamente a los artículos 24 y 25 del RGPD, pues establece: “*Cuando el sistema afecte a datos personales, la adopción de medidas de mínimo privilegio y desde el diseño deberá realizarse de acuerdo con los artículos 24 y 25*” del RGPD.

La remisión que el **artículo 5** del proyecto hace en las letras **b)** y **h)** a los artículos 24 y 25 del RGPD determina que la PSI que se informa, en el caso de que un sistema de información trate datos personales, prevé expresamente “*aplicar*” medidas técnicas y organizativas adecuadas, adoptadas tras la valoración de diversos factores, particularmente del riesgo que el tratamiento represente para los derechos y libertades de las personas físicas, cuya finalidad será garantizar y poder demostrar que el tratamiento es conforme con

el RGPD y garantizar de forma efectiva los principios que rigen el tratamiento de datos integrando las garantías en el tratamiento.

Las reglas del **artículo 5** del proyecto a las que se hace mención en los párrafos precedentes revelan que **la orden proyectada**, en relación con el tratamiento de datos de carácter personal, **ha incorporado una visión de la gestión de riesgos conjunta e integrada con los sistemas de información**.

Por lo que respecta a los “*incidentes de seguridad*” (requisito mínimo que debe desarrollar la PSI, de acuerdo con el artículo 12.6.m, del ENS) el **artículo 5** del proyecto regula esta materia en dos apartados, las letras **n)** y **o)**.

En el primero de ellos, “*Incidentes de seguridad*”, letra **n)**, la orden establece que la reacción ante incidentes de seguridad comprenderá procedimientos de actuación que contemplen medidas de detección, la notificación oportuna, los protocolos para el intercambio de información relacionada con el incidente, medidas de restauración de la información y de los servicios y “*la disposición de los medios necesarios para garantizar la recuperación efectiva de los servicios más críticos en el tiempo máximo tolerable*”.

En la letra **o)** el **artículo 5** contempla, específicamente, **la gestión de incidentes de seguridad que afecten a datos de carácter personal**. Y en relación con ellos esta norma remite al RGPD y a la LOPDGDD, en especial a su disposición adicional primera.

Así, el párrafo segundo del **artículo 5.o)** menciona expresamente la obligación de notificar el incidente a la autoridad de control (ex artículo 33 del RGPD), de comunicación al interesado (ex artículo 34 RGPD) y la obligación de documentar el incidente de seguridad (ex artículo 33.5 RGPD)

Por último, el **registro de actividad** de las personas usuarias al que alude la letra **m)** del **artículo 5** del proyecto, es objeto de un análisis independiente en un epígrafe específico.

En consideración a lo expuesto, se aprecia que el **artículo 5** del proyecto de orden, relativo a los requisitos de seguridad de la información, es acorde con la normativa de protección de datos de carácter personal por lo que **se informa favorablemente, con una salvedad que atañe al inciso último del último párrafo del apartado b)** del precepto.

IV

El artículo 3, apartado 3, del ENS dispone: “*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.”

Este precepto tiene su origen en la disposición adicional primera de la LOPDGDD, “*Medidas de seguridad en el ámbito del sector público*”, que indica en el apartado 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”.

Pues bien, la norma que se informa recoge expresamente en su **artículo 15.1** la prevalencia frente al ENS de las medidas de seguridad agravadas que sean fruto del análisis de riesgos y, en su caso, de la evaluación de impacto efectuada con arreglo al RGPD.

El sentido de la disposición del artículo 3.3 del ENS no plantea ninguna duda interpretativa. Los términos de la comparación son, de una parte, las medidas que conforme al artículo 32 del RGPD resulten adecuadas para garantizar la seguridad de los datos personales, a la vista del análisis de riesgos y, en su caso, de la evaluación de impacto del tratamiento, y, de otra, el “*Anexo II, Medidas de Seguridad*”, del ENS, que incluye una relación de medidas y de criterios para su determinación.

A tal efecto se advierte que el **último inciso** del **último párrafo** de la letra **b)**, “*Análisis y gestión de los riesgos*”, del **artículo 5** del proyecto, **priva de sentido** a dicho párrafo. El precepto dispone:

“El análisis y la gestión deberá realizarse de acuerdo con las previsiones del artículo 15 de la presente orden ministerial, adaptando los criterios de determinación del riesgo en el tratamiento de los datos conforme a lo establecido en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y, en caso necesario, estableciendo niveles de seguridad más altos.”

La disposición transcrita, con su actual redacción, significa que podrán establecerse niveles de seguridad más altos que los previstos en el artículo 32 del RGPD. Afirmación que carece de lógica teniendo en cuenta que el RGPD no contiene (a diferencia del ENS) un catálogo de medidas de seguridad, sino que se refiere a las medidas de seguridad “*apropiadas para garantizar un nivel de seguridad adecuado al riesgo*”. Por las razones apuntadas, **se sugiere suprimir el último inciso** (“*y, en caso necesario, estableciendo niveles de seguridad más altos*”) del párrafo último del artículo 5.b) del proyecto.

Como se ha indicado, el proyecto normativo sí incorpora, a través de su artículo 15, “*Tratamiento de datos personales*”, apartado 1, la previsión del artículo 3.3 del ENS.

El artículo 15.1 del proyecto establece que, cuando se traten datos de carácter personal, se adoptarán (a tenor del artículo 32 del RGPD) las medidas de seguridad que resulten apropiadas en consideración al análisis de riesgos efectuado conforme al artículo 24 del RGPD y a la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales de acuerdo con el artículo 35 del RGPD.

Y añade —último párrafo del apartado 1 del artículo 15— que, cuando el resultado de esas operaciones **“*determine*” medidas de mayor gravedad que las recogidas en el anexo II del Real Decreto 311/2022, serán aquellas medidas las que se aplicarán** para garantizar la protección de los datos personales. El artículo 15.1 de la orden dispone:

“1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Trabajo y Economía Social las medidas de seguridad apropiadas derivadas del análisis de riesgos de privacidad, así como de la evaluación de impacto relativa a la protección de datos, tal y como se detalla en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. [...]

En el caso de que el análisis de riesgos y la evaluación de impacto en su caso, determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de mayo, dichas medidas serán las que se implementarán en la protección de datos personales.”

Así pues, **se valora favorablemente el artículo 15.1 de la orden proyectada** que, siguiendo el artículo 3.3 del ENS, prevé que las medidas de seguridad que se implanten de acuerdo con el artículo 32 del RGPD, como consecuencia del análisis de riesgos y eventualmente de una evaluación de impacto, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberán prevalecer sobre éstas últimas a fin de que el nivel de seguridad que se garantice sea el adecuado al riesgo que entrañen para los derechos y libertades de las personas físicas los tratamientos de datos de carácter personal que esté previsto efectuar.

V

El proyecto encomienda la *gestión de la seguridad* de los sistemas de información del MTES a *una estructura organizativa* descrita en su **artículo 6**, compuesta por un total de nueve agentes entre los que figuran (apartados **g**, y **h**, respectivamente) las *personas responsables* y las *personas encargadas del tratamiento* de datos de carácter personal.

Cabe indicar, además, que la orden proyectada incorpora el principio de “*Diferenciación de responsabilidades*” previsto en el artículo 5.g) del ENS.

El **artículo 4** del proyecto, “*Principios de la Política de Seguridad*”, en su apartado **h)**, “*Función diferenciada*”, dispone que el MTES “*organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.*”

El precepto añade que, en los supuestos de *tratamientos de datos personales*, se identificará a la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado de tratamiento, “*de acuerdo con los dispuesto en el artículo 4, apartados 7 y 8 del RGPD.*”

De este último párrafo del **artículo 4.h)** se infiere que la orden hace suya la definición de *responsable del tratamiento* y de *encargado del tratamiento* contenida en el RGPD (artículo 4, apartados 7 y 8 respectivamente).

También, el artículo **5**, letra **a)** del proyecto, relativo a los requisitos mínimos de la seguridad de la información, previene que “*La seguridad deberá comprometer a todo el personal del Ministerio de Trabajo y Economía Social*”.

Por lo que respecta al “*rol*” que la orden asigna al responsable y al encargado del tratamiento en la gestión de la seguridad de la información, éste puede extraerse (habida cuenta de que el proyecto no dedica un precepto específico a regular esas figuras) de algunas de las normas que integran el proyecto.

En particular, el **artículo 5.b)**, **segundo párrafo**, del proyecto normativo encomienda al responsable del tratamiento realizar un análisis de riesgos conforme al artículo 24 del RGPD y una evaluación de impacto en la protección de datos “*en los supuestos de su artículo 35*”. El precepto establece:

“Cuando un sistema de información trate datos personales, la persona responsable o encargada del tratamiento, asesorada por la persona delegada de protección de datos, realizará 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.”

Puede concluirse de lo expuesto que la concepción que el proyecto tiene de la figura del responsable y del encargado del tratamiento y las funciones que

les encomienda **es plenamente acorde con la normativa reguladora del derecho fundamental a la protección de datos de carácter personal.**

En cuanto al resto de los sujetos que forman parte de la estructura organizativa encargada de gestionar la seguridad de la información, la orden dedica a su regulación los artículos 7 a 14.

El artículo 7 *redefine* el Comité de Seguridad de las Tecnologías de la Información y de las Comunicaciones (COSTIC) como órgano colegiado de carácter transversal adscrito a la Subsecretaría de Estado de Trabajo y Economía Social. Se compone de una presidencia, una vicepresidencia y diez vocalías.

Es digno de mención que son vocales del COSTIC, entre otros sujetos, la persona responsable de la seguridad del MTES (5ª); la persona responsable de la seguridad del Servicio Público de Empleo Estatal, SEPE, (6ª); la persona responsable de la seguridad del Fondo de Garantía Salarial, FOGASA (7ª); la persona responsable de la seguridad del Instituto Nacional de la Seguridad y Salud en el Trabajo, INSST (8ª); la persona responsable de la seguridad del Organismo Estatal de la Inspección de Trabajo y Seguridad Social, OEITSS (9ª) y la persona responsable de la seguridad del Consejo Económico y Social, CES (10ª).

Entre las funciones que el **artículo 8** encomienda al COSTIC se menciona, letra g), *“Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y, en particular, en materia de protección de datos de carácter personal”*.

El **artículo 10** está dedicado a la figura del responsable del sistema, definida como *“la persona que tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida”*. Entre las funciones encomendadas, el **artículo 10.2.b)** refiere la de *“Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.”*

El **artículo 11** del proyecto se ocupa del responsable de la información, del que dice que *“tiene la potestad de establecer los requisitos de la información tratada y su implicación en la valoración del sistema de información del que forme parte.”* Entre las funciones encomendadas, el artículo **11.2**, letras **b)** y **c)**, refieren *“Valorar el impacto que tendría un incidente que afectase a la seguridad de la información con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad”* y *“La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el*

cumplimiento de sus obligaciones de servicio y el respeto de la legalidad y de los derechos de los ciudadanos.”

Por último, el artículo 12 está dedicado al responsable de los servicios, sobre el que indica que *“tiene la potestad de establecer los requisitos del servicio prestado y su implicación en la valoración del nivel de seguridad de dicho servicio.”*

Y en cuanto al responsable de la seguridad, el artículo 13 del proyecto lo define como la persona *“que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos y reportar sobre estas cuestiones”*.

Finalmente, con el propósito de diferenciar con nitidez las figuras que el artículo 6 del proyecto integra en su estructura organizativa y delimitar las funciones que corresponden, de una parte, al responsable y encargado del tratamiento, y de otra al COSTIC, al responsable del sistema y al responsable de la información, procede traer a colación el Informe 170/2018 del Servicio Jurídico de la AEPD en el que se examina 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”. Dice el citado Informe:

“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.

[...].

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.

[...]

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. [...]

[...]

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)”.

VI

El proyecto incluye en la estructura organizativa a la que se encomienda la gestión de la seguridad de la información en su ámbito de aplicación a la “*persona designada como Delegado/a de Protección de Datos*” (en lo sucesivo, el DPD), **artículo 6.f)**.

No obstante, la regulación que el proyecto hace del DPD es respetuosa con la independencia con la que el RGPD la caracteriza y con las funciones esenciales que le encomienda. En ese sentido, el **artículo 14.1** del proyecto, “*Delegado o delegada de protección de datos*”, dispone que se deberá garantizar su independencia dentro de la organización y evitar cualquier conflicto de intereses.

El RGPD dedica los artículos 37 a 39 a la regulación de esta figura. El artículo 38 del RGPD establece 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.*”

A tenor del artículo 39 del RGPD “*El delegado de protección de datos tendrá como mínimo las siguientes funciones:*

a) 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;

b) 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;

c) 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;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2.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.”

En idéntico 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 y revisado el 5 de abril de 2017 (documento WP243), subraya 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”*.

El proyecto dedica al DPD un precepto específico (**artículo 14**, *“Delegado o delegada de protección de datos”*) y también se refiere a él en varias de sus disposiciones: el **artículo 5.b)**, *“Análisis y gestión de los riesgos”*, párrafo segundo, menciona expresamente el asesoramiento que el DPD presta al responsable o encargado de tratamiento cuando el sistema de información trate datos personales con ocasión de que aquél lleve a cabo un análisis de riesgos conforme al artículo 24 del RGPD o una evaluación de impacto en la protección de datos en los supuestos del artículo 35 del RGPD.

En términos similares, el **artículo 15**, *“Tratamiento de datos personales”*, **apartado 1, párrafo segundo**, indica que cuando un sistema de información trate datos personales, la persona del responsable o la persona encargada de tratamiento, asesoradas por el DPD, realizarán un análisis de riesgos conforme al artículo 24 del RGPD.

Además, el **artículo 15.2** del proyecto, prevé que se establezca *“la oportuna coordinación”* con la persona designada como DPD, de una parte, con las personas responsables y con las encargadas del tratamiento de datos personales, de otra, *“En función de las diversas situaciones que puedan producirse en materia de protección de datos personales”* *“y en la medida en que sea preciso”*. El párrafo segundo del **artículo 15.2** del proyecto añade: *“Especialmente, se prestará apoyo a la persona designada como delegada de protección de datos, para la elaboración de propuestas o informes relativos a las reclamaciones de los interesados, comunicación de brechas de datos personales y respuestas a los requerimientos de la Agencia Española de Protección de Datos.*

Es exponente de la función asesora que el artículo 39 del RGPD encomienda al DPD **el artículo 7 del proyecto** que, con ocasión de regular el COSTIC, dice en su **apartado 2** que la persona designada como DPD *“participará con voz, pero sin voto”* en sus reuniones, cuando vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal y siempre que se requiera su participación. Disposición que salvaguarda la independencia del DPD al tiempo que le permite desempeñar su función asesora.

El **artículo 14** del texto insiste en el carácter asesor del DPD. En ese sentido, su apartado 1 dispone que tiene *“carácter asesor y supervisor para el cumplimiento de los dispuesto en el RGPD”* y demás normativa sobre protección de datos personales *“debiéndose garantizar su independencia dentro de la organización y evitar cualquier conflicto de intereses, así como proveer de los medios necesarios para el desarrollo de sus funciones conforme al artículo 39 del mencionado Reglamento.”*

La función asesora y supervisora que se atribuye al DPD se extiende, dice el **apartado 2 del artículo 14**, a *“aquellas aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.”*

El **apartado 3 del artículo 14** versa sobre la intervención del DPD en la *“gestión de las brechas de datos personales, principalmente en su posición de interlocutor de la persona responsable o encargada del tratamiento”* ante la AEPD. En este aspecto, es importante reiterar que la intervención del DPD en las brechas de datos personales será, en su caso, la de interlocutor ante la autoridad de control. Aclaración que parece necesaria visto el equívoco que pudiera desprenderse del tenor literal del **artículo 15.2** del proyecto, segundo párrafo, que parece atribuir al DPD las comunicaciones de brechas, cuando conforme al artículo 33 del RGPD la comunicación a la autoridad de control de una brecha de datos personales constituye una obligación del responsable del tratamiento y en ningún caso del DPD.

Así pues, las previsiones que sobre el DPD constan en el proyecto (artículos 5.b, párrafo segundo; 7.2; 15.2 y artículo 14) **merecen una valoración favorable**.

No obstante, se **sugiere** incluir en el texto de la orden proyectada una referencia a las previsiones del artículo 37.5 del RGPD, relativas a las cualidades profesionales, conocimientos especializados y capacidad del candidato que determinarán la designación del DPD, máxime cuando en el ámbito de esta PSI es preceptivo su nombramiento conforme al artículo 37.1.a) del RGPD.

Igualmente, se aconseja incorporar al texto del proyecto el artículo 38.3 del RGPD que concreta cuál es la “*Posición del delegado de protección de datos*” y que dispone: “*El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado*”

VII

El artículo 24 del ENS, “*Registro de actividad y detección de código dañino*”, establece:

1. *Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, 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.*
2. *Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.*
3. *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.*

El proyecto que se informa dispone en el **artículo 5,m)**, “*Registro de actividad*”:

“Se habilitarán registros de la actividad de las personas usuarias 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 con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones que resulten de aplicación.”

La disposición transcrita es una copia del artículo 24 apartado 1 del ENS, relativo al “registro de actividad”, y de su apartado 3. Los registros de la actividad de las personas usuarias que habilita el ENS permiten retener la “información necesaria” (la información “*estrictamente necesaria*” dice el artículo 24.1 del ENS) para las finalidades que se mencionan (monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas) debiendo respetar la normativa de protección de datos de carácter personal.

Así pues, **se informa favorablemente el artículo 5.m)** del proyecto.

La PSI del MTES sometida a informe **no contiene ninguna disposición que incorpore la previsión del artículo 24.2 del ENS**, norma que habilita a realizar un tratamiento de datos de carácter personal que consiste en “*analizar las comunicaciones entrantes o salientes*” “*para una finalidad específica*”: “*la seguridad de la información*”, “*la seguridad de los sistemas de información*” para garantizar “*la rigurosa observancia de los principios de actuación de las Administraciones públicas*”.

Un tratamiento con tal finalidad permitiría (i) impedir el acceso no autorizado a las redes y sistemas de información, (ii) detener los ataques de denegación de servicio, (iii) evitar la distribución malintencionada de código dañino y (iv) otros daños a las antedichas redes y sistemas de información.

Además, el tratamiento así definido únicamente podría llevarse a cabo “*en la medida estrictamente necesaria y proporcionada*”, pues lo exige expresamente el artículo 24.2 del ENS que requiere que el tratamiento –“*analizar las comunicaciones entrantes o salientes*”— sea “*proporcionado*” a la finalidad que persigue (la seguridad de la información) y limitado a lo necesario para cumplir dicha finalidad. Y exige también (artículo 24.2 del ENS) que un tratamiento de esa naturaleza observe estrictamente los principios de limitación de la finalidad, minimización de datos y limitación del plazo de conservación y cumpla el resto de las disposiciones del RGPD.

En el proyecto normativo que se informa la única disposición que tangencialmente podría relacionarse con la previsión del artículo 24.2 del ENS es el **apartado 2 de su artículo 14**, dedicado a regular el DPD, que establece:

“El asesoramiento y supervisión del delegado de protección de datos se extiende a aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.”

Sin embargo, **no puede admitirse que tal disposición de la orden que se informa acoja la previsión del artículo 24.2 del ENS, con la consecuencia que la PSI del MTES no contempla la posibilidad de que se analicen las comunicaciones entrantes o salientes para los fines de seguridad de la información a los que alude el precepto citado.**

Al hilo de lo expuesto recordamos que uno de los principios básicos del ENS es la “*Seguridad como proceso integral*” (artículo 5.a, del Real Decreto 311/2022). Como explica el artículo 6.1. del citado RD 311/2022, se trata de un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. Y añade que “*La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.*”

VIII

En síntesis, la norma proyectada merece un juicio favorable con algunas puntualizaciones necesarias.

Se valora positivamente el **artículo 4** del proyecto, relativo a los principios básicos de la política de seguridad, acorde con la normativa de protección de datos de carácter personal, del que se destaca su propósito de integrar en la política de seguridad del MTES las exigencias inherentes a la normativa reguladora del derecho fundamental que nos ocupa.

Idéntico juicio favorable se hace del **artículo 5** del proyecto, relativo a los requisitos de seguridad de la información, incluida la letra **m)** sobre el registro de actividad, con una importante matización: **se sugiere suprimir el último inciso del último párrafo** de la letra **b)**, “*Análisis y gestión de los riesgos*”, del **artículo 5** del proyecto, por cuanto tal inciso priva de sentido al párrafo en el que está incardinado.

Se informa favorablemente el artículo 15.1 del proyecto, que acoge el artículo 3.3 del ENS y prevé que las medidas de seguridad que se implanten de acuerdo con el artículo 32 del RGPD, como consecuencia del análisis de riesgos y eventualmente de una evaluación de impacto, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberán prevalecer sobre éstas últimas.

La concepción de la figura del responsable y del encargado del tratamiento y de sus funciones en la norma proyectada se estima que es respetuosa con el RGPD y la LOPDGDD. Para delimitar estas figuras de otros sujetos previstos en el ENS que el proyecto regula y diferenciar las funciones que corresponden a unos y otros, se reproducen las consideraciones del Informe 170/2018 del Servicio Jurídico de la AEPD sobre la diferenciación sustantiva y competencial que existe entre el ámbito de la seguridad de la información y el de la protección de datos de carácter personal.

Merece, asimismo, un juicio favorable la regulación de la figura del DPD. Pese a lo cual, se **sugiere** incluir en el texto (artículo 14) una referencia a las cualidades profesionales que debe reunir la persona designada, de acuerdo con el artículo 37.5 del RGPD, a la posición del delegado de protección de datos y a la garantía de independencia en el desempeño de sus funciones a tenor del artículo 38.3 del RGPD.

Por último, el informe destaca la **ausencia de regulación** en el proyecto de la previsión del artículo 24.2 del ENS de “**detección de código dañino**”.