

N/REF: 0040/2025

I

De acuerdo con su artículo 1, constituye el objeto del texto sometido a informe la Política de Seguridad de la Información (PSI) correspondiente a los servicios centrales (SSCC) del Ministerio de Política Territorial y Memoria Democrática (MPTMD) en el ámbito de la Administración Electrónica y de la protección de datos personales y su marco organizativo y tecnológico.

Sobre el ámbito subjetivo de aplicación de la PSI los párrafos segundo y tercero del artículo 1 del proyecto de Orden establecen:

“Conforme al Real Decreto 273/2024, de 19 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Memoria Democrática, el ámbito subjetivo de esta Política aplicará a los SSCC del MPTMD.”

“La Política de Seguridad de los SSCC aprobada mediante orden ministerial será de obligado cumplimiento para todos los órganos superiores y directivos de los SSCC, siendo aplicable a todos los sistemas de información de éstos y, en general, a toda la información que sea gestionada por el departamento, con independencia de cuál sea su soporte, destino, adscripción o relación con el mismo, así como a toda aquella persona que acceda a ella.”

A ese respecto, la memoria de análisis de impacto normativo (MAIN) que acompaña al proyecto de Orden explica que los sistemas de información de los servicios periféricos de las Delegaciones, Subdelegaciones del Gobierno y Direcciones Insulares *“requieren una política de seguridad separada”* por revestir una especial complejidad dado que parte de los sistemas y de la propia información dependen o se integran en sistemas de otros departamentos ministeriales.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), exige (artículo 12.3) que en la Administración General del Estado cada ministerio cuente con su política de seguridad que aprobará la persona titular del Departamento. De manera que la Orden proyectada cumple el mandato del artículo 12.3 del ENS y los principios de buena regulación de necesidad y eficacia, al ser el instrumento utilizado (Orden Ministerial) el adecuado para su cumplimiento.

Asimismo, dispone el artículo 12 del ENS, apartado 6, que la PSI *“se establecerá de acuerdo con”* los *principios básicos de seguridad* de la información recogidos en el capítulo II (seguridad como proceso integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua; reevaluación periódica y diferenciación de

responsabilidades) y “se desarrollará aplicando” los *requisitos mínimos* contemplados en dicho precepto: a) Organización e implantación del proceso de seguridad; b) Análisis y gestión de los riesgos; c) Gestión de personal; d) Profesionalidad; e) Autorización y control de los accesos; f) Protección de las instalaciones; g) Adquisición de productos de seguridad y contratación de servicios de seguridad; h) Mínimo privilegio; i) Integridad y actualización del sistema; j) Protección de la información almacenada y en tránsito; k) Prevención ante otros sistemas de información interconectados; l) Registro de la actividad y detección de código dañino; m) Incidentes de seguridad; n) Continuidad de la actividad y ñ) Mejora continua del proceso de seguridad.)

El proyecto que se informa da cumplimiento a la previsión del artículo 12.6 del ENS pues su **artículo 5** incorpora y desarrolla los *principios básicos de la seguridad* de la información y dispone que bajo tales principios el MPTMD implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y de los servicios a proteger teniendo en cuenta la categoría de los sistemas afectados. Además, el **artículo 6** del proyecto normativo recoge los *requisitos mínimos de seguridad* de la información a los que alude el artículo 12.6 del ENS.

Los **artículos 7 a 12** de la norma proyectada están dedicados a la estructura organizativa de la PSI de los SSCC del MPTMD que quedaría integrada por los siguientes agentes a los que compete mantenerla, actualizarla y hacerla cumplir: (i) el Comité de Seguridad de la Información (CSI); (ii) el Responsable de Seguridad de la Información; (iii) el Responsable de la Información, del Servicio y del Tratamiento; (iv) el Responsable del Sistema y (v) el responsable y el encargado del tratamiento de datos personales.

II

Centrándonos en la protección de los datos de carácter personal corresponde hacer mención, en primer término, al artículo 3 del Esquema Nacional de Seguridad, “*Sistemas de información que traten datos personales*”, que establece:

“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.”

El precepto del ENS transcrito, para el caso de que un sistema de información trate datos personales, hace una remisión 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 subraya el Preámbulo de la LOPDGDD y así lo han reflejado en numerosas ocasiones los informes del Servicio Jurídico, el RGPD representa la evolución de un modelo basado en el control del cumplimiento a otro que descansa en el principio de responsabilidad proactiva. Sus preceptos exigen una previa valoración por el responsable o por el encargado del tratamiento del riesgo para los derechos y libertades de las personas físicas que pudiera generar el tratamiento de los datos de carácter personal para que, a partir de dicha valoración, se adopten las medidas que procedan.

En tal sentido, el Informe N/REF:0103/2022, tomando en consideración el nuevo modelo de cumplimiento que representa el RGPD, basado en la responsabilidad activa, 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 estas ya no establecen un modelo tasado de cumplimiento.”*

Recordemos que el RGPD ha establecido el principio de responsabilidad proactiva (ex artículo 5.2) en virtud del cual el responsable del tratamiento será responsable de cumplir los principios que presiden el tratamiento de datos recogidos en el artículo 5.1 y capaz de demostrarlo, debiendo adoptar a tal fin las 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 entraña 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). 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). 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).

El proyecto de Orden acoge el pleno sometimiento de los tratamientos de datos que se efectúen en su ámbito aplicación a la normativa reguladora de protección de datos de carácter personal.

A ese respecto, el mismo **preámbulo del proyecto normativo** (párrafo sexto) nos recuerda que el “RGPD señala que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos de dicho Reglamento. A fin de poder demostrar la conformidad con el RGPD, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto”.

El **artículo 3** de la Orden proyectada -relativo al marco normativo en el que se desarrollan las actividades de los SSCC del MPTMD en el ámbito de la prestación de los servicios electrónicos a la ciudadanía- relaciona entre ellas, en primer lugar, el RGPD y la LOPDGDD.

El **artículo 5**, “Principios de la seguridad de la información”, es también un exponente de que el proyecto informado es acorde con el RGPD.

El precepto citado sigue en esencia la regulación sobre los principios básicos de seguridad que contiene el Real Decreto 311/2022 en su capítulo II, artículos 5 a 11. El ENS relaciona en el artículo 5, apartados a) a g), los “Principios básicos del Esquema Nacional de Seguridad” y los desarrolla en los artículos siguientes, dedicando 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 5** del proyecto normativo comienza señalando que la PSI 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 complejidad de la materia regulada. A continuación, dispone que las medidas de seguridad -que serán proporcionales a la naturaleza de la información y de los servicios a proteger- se implementarán bajo los siguientes principios:

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. La seguridad constituirá un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

d) Análisis y gestión de riesgos: Todos los sistemas afectados por la PSI de los SSCC del MPTMD, 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 de 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 RGPD, el artículo 28 de la**

LOPD 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 mejora continua. Se implementará un proceso integral de prevención, reacción y recuperación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

f)Líneas de defensa. Se implementará una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permitirá ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse; reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

g)Reevaluación periódica e integridad y actualización del sistema. Se implementarán controles y evaluaciones regulares y periódicas de la seguridad (de forma interna o con la ayuda de terceros) para conocer en todo momento el estado de la seguridad de los sistemas con el objeto de adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

h)Función diferenciada: MPTMD organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el artículo 6. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

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 RGPD.

A través del **apartado a) del artículo 5** el proyecto de Orden incorpora a la PSI 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 **apartado a) del artículo 5** del proyecto dice que estarán destinadas a garantizar *el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal.* Párrafo 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.”*

Esto, porque el artículo 16 de la Orden proyectada, *“Protección de datos de Carácter Personal”* dispone en su párrafo tercero:

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

El **apartado b) del artículo 5** del proyecto - *“Análisis y gestión de riesgos”*-, de acuerdo con el RGPD, obliga a que todos los tratamientos de datos personales que se efectúen en su marco de aplicación sean objeto de un análisis de riesgos:

“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.”

Para el precepto (apartado b, del artículo 5 del proyecto) el objeto del análisis de riesgos es *“evaluar las amenazas y los riesgos a los que están expuestos”* los tratamientos de datos. No recoge una mención expresa a los riesgos *para los derechos y libertades de los interesados* como sí hace el RGPD. No obstante, tal omisión es irrelevante porque otras disposiciones del proyecto de Orden hacen una remisión a los artículos 24 y 25 del RGPD. Así, el artículo 6, *“Requisitos de seguridad de la información”*, dispone en el apartado h): *“Cuando el sistema afecte a datos personales, la adopción de medidas de seguridad por defecto y desde el diseño deberá realizarse de acuerdo con los artículos 24 y 25 del RGPD.”*

Por otra parte, el **apartado b) del artículo 5** del proyecto exige que el análisis de riesgos se ajuste *“en todo caso, a un criterio de proporcionalidad de los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados”*.

Esta previsión del proyecto informado 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.”*

Cabe destacar que el **apartado d) del artículo 5** del proyecto de Orden incluye criterios temporales para llevar a cabo el análisis de riesgos *“cuando el sistema de*

información trate datos personales”, apoyándose –“de acuerdo”, dice la norma- en los artículos “24,25 y 32 del RGPD, el artículo 28 de la LOPD y el artículo 3 del RD311/2022”.

En este sentido, recordamos que 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.”* Que el artículo 25 del RGPD menciona el *“momento de determinar los medios de tratamiento”* y el *“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 que 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.”*

Pues bien, el **artículo 5.d)** del proyecto de Orden establece que el análisis de riesgos se efectúe 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.

Este precepto del proyecto es plenamente acorde con la normativa de protección de datos de carácter personal 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*. Sobre tal cuestión resultan muy esclarecedores los epígrafes 37 y 38 de las Directrices 4/2019 del 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.”

En consideración a lo expuesto **informamos favorablemente el contenido del artículo 5** del proyecto de Orden que es objeto de análisis 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 refiere en la letra b) el *“Análisis y gestión del riesgo”*.

El **artículo 6** del proyecto, *“Requisitos de Seguridad de la Información”*, en su **apartado b)**, *“Análisis y gestión de los riesgos”*, concibe la gestión del riesgo como un proceso consistente en la *“identificación, análisis, evaluación y tratamiento a los que el sistema esté expuesto.”* Añade 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, en parte, el artículo 14 del ENS.

El **apartado b)** del **artículo 6** contiene normas específicas sobre el análisis y gestión de los riesgos para el caso de que el tratamiento afecte a datos de carácter personal. Establece que cuando el sistema 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 General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos”*

Añade que la gestión del riesgo se efectuará de acuerdo con su artículo 14, *“adaptando los criterios de determinación del riesgo en el tratamiento de los datos”* a lo establecido en el artículo 32 del RGPD y, en caso necesario, estableciendo niveles de seguridad más altos.

Por otra parte, en relación con las medidas que deben adoptarse, el **artículo 6** del proyecto, letra **h)**, 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 seguridad por defecto y desde el diseño deberá realizarse de acuerdo con los artículos 24 y 25 del RGPD.”*

La remisión que el **artículo 6** del proyecto hace en las letras **b) y h)** a los artículos 24 y 25 del RGPD implican que, para el caso de sistema de información que traten datos personales, la PSI que se informa se obliga expresamente a “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 normas del artículo 6 del proyecto a las que se ha hecho mención revelan que la Orden proyectada ha incorporado una visión conjunta e integrada de la gestión de riesgos en los sistemas de información cuando traten datos de carácter personal.

Respecto al requisito de seguridad previsto en el apartado e) del artículo 12 del ENS, Autorización y control de los accesos, el artículo 6 del proyecto se refiere a él en la **letra d) del artículo 6**.

Esta disposición no menciona expresamente el tratamiento de datos de carácter personal pero sí previene que *“Los sistemas de información individuales se diseñarán de forma que garanticen la seguridad por defecto, proporcionando la mínima funcionalidad requerida para alcanzar los objetivos y priorizando el uso sencillo, de tal forma que una utilización insegura requiera, en todo caso, de un acto consciente por parte del usuario.”*

El apartado **g)** del **artículo 6** reitera la referencia a la “*seguridad por defecto*” estableciendo que *los sistemas deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto*.

El **artículo 6** se refiere en el **apartado j)** a la “*Protección de la información almacenada y en tránsito*” indicando que se implementarán mecanismos para proteger la información almacenada o en tránsito, especialmente cuando ésta se encuentra en entornos inseguros. Norma que debe conectarse, desde el punto de vista de la protección de datos de carácter personal, con el artículo 5 apartado a) del proyecto que establece que *“Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal.”*

Respecto a los “*incidentes de seguridad*” (artículo 12, m del ENS) el **artículo 6** del proyecto, **letras n)** y **o)** se refiere expresamente al tratamiento de datos de carácter personal. De una parte, la **letra n)** dice que se tendrá en cuenta en la “*gestión de incidentes que afecten a datos personales*” lo dispuesto en el RGPD y en la LOPDGDD, y añade “*en especial su disposición adicional primera*”, y el resto de normativa aplicable.

La letra **o)** hace referencia expresa a la obligación de notificación del 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)

Las cuestiones relativas a los registros de actividad de las personas usuarias (que se incluye como **letra l) en el artículo 6 y el apartado s)**, referente al uso de herramientas de IA generativa externa, son objeto de un análisis independiente en un epígrafe específico.

En conclusión, conforme a lo expuesto, y con la salvedad hecha para los apartados l) y s) del artículo 6, se informa favorablemente el contenido de este precepto relativo a los requisitos de seguridad de la información.

IV

El artículo 3 del ENS, apartado 3, transcrito en los epígrafes precedentes, establece que *“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.”

El precepto tiene su origen en la Disposición Adicional primera de la LOPDGDD que en su apartado 1 señala que *“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”*.

El proyecto informado alude en varios de sus artículos a la prevalencia frente al ENS de las medidas de seguridad agravadas que son fruto del análisis de riesgos y, en su caso, de la evaluación de impacto efectuada con arreglo al RGPD.

Así, el **artículo 6** de la Orden proyectada, *“Requisitos de seguridad de la información”*, contempla la posibilidad de establecer niveles de seguridad más altos de los previstos por el ENS como consecuencia de determinar el riesgo del tratamiento con arreglo a los artículos 24 y 32 del RGPD y dispone en su **apartado b)** *“Análisis y gestión de los riesgos”*:

“1.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.

2.El análisis y la gestión deberá realizarse de acuerdo con las previsiones del artículo 14 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 RGPD y, en caso necesario, estableciendo niveles de seguridad más altos.”

Con más rotundidad el **artículo 16** del proyecto que se informa, *“Protección de Datos de Carácter Personal”*, dice en sus **tres primeros párrafos**:

“Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Política Territorial y Memoria Democrática, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de la evaluación de impacto relativa a la protección de datos, que se detalla en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de carácter Personal y Garantía de Derechos Digitales.

Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en las medidas del citado Anexo, las medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

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

Asimismo, el **artículo 14** de la propuesta normativa, “Gestión de los riesgos”, dice en su último párrafo:

“En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo 16, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del Delegado de Protección de Datos, se puedan añadir a los establecidos conforme al Real Decreto 311/2022, de 3 de mayo, si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales fuesen de alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de Protección de Datos (AEPD). En este aspecto, también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD.”

Resulta de la exposición precedente que, tal y como ha venido informando esta Agencia, las medidas a implantar como consecuencia del análisis de riesgos previsto en el artículo 32 del RGPD, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberán prevalecer sobre éstas últimas a fin de que el nivel de seguridad sea adecuado al riesgo que los tratamientos de datos suponen para los derechos y libertades de las personas, como exige el RGPD.

En consecuencia, **se valora favorablemente el artículo 16 del proyecto informado, así como los artículos 6 y 14, que prevén que cuando el análisis de riesgos determine medidas agravadas respecto a las previstas en el Anexo del Esquema Nacional de Seguridad serán las medidas derivadas de dicho análisis las que deban implementarse en aras de la protección de datos de carácter personal con arreglo al RGPD.**

V

El proyecto normativo atribuye la gestión de la seguridad de la información en el ámbito de la PSI de los SSCC del MPTMD a una estructura organizativa descrita en su **artículo 7** -citado en el epígrafe I de este Informe- compuesta por diversos agentes -un total de cinco- entre los que se incluyen (apartado e) los “Responsables y encargados del tratamiento de datos personales”.

El proyecto dedica el **artículo 12** a los responsables y encargados de tratamiento y concibe ambas figura en términos idénticos al RGPD.

Así, el **artículo 12** del proyecto -coincidiendo, salvo en su último inciso, con el artículo 4.8 del RGPD- establece que *“El responsable de tratamiento es la persona física o jurídica, autoridad pública, servicio u otra entidad que, solo o junto con otros, determina los fines y medios del tratamiento y aplica las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa vigente en materia de protección de datos personales.”* En cuanto al encargado de tratamiento, la definición del artículo 12 del proyecto es una transcripción del artículo 4.8 del RGPD.

Añade el artículo 12 del proyecto informado que *“La identidad del responsable de tratamiento figura en el registro de las actividades de tratamiento efectuadas bajo su responsabilidad, de acuerdo con lo dispuesto en el artículo 30 del Reglamento General de Protección de Datos”*

El **artículo 5.h)** de la Orden proyectada, *“Función diferenciada”*, acoge el principio de *“Diferenciación de responsabilidades”* establecido en el artículo 5.g) del ENS.

El mencionado **apartado h) del artículo 5** previene que el MPTMD *“organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el artículo 6. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.”* Y 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 lo dispuesto en el artículo 4, apartados 7 y 8 del RGPD.

Se examina por ello cuál es el “rol” que el proyecto normativo asigna en la gestión de la seguridad de la información al responsable y al encargado del tratamiento y si éste se adecúa a la normativa de protección de datos de carácter personal.

El **artículo 6.b) 1º** del proyecto 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:

“1.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.”

En conclusión, **la concepción de la figura del responsable y del encargado del tratamiento y las funciones que se les encomiendan en el proyecto es plenamente respetuosa con la normativa específica, por lo que se informan favorablemente sus artículos 12 y 6.1.b).**

La Orden que se informa regula el resto de los sujetos o agentes que integran la estructura organizativa de la PSI de los SSCC del MPTMD, entre ellos los Responsables del Servicio y de la Información (artículos 10 y 14) cuyas funciones *aparentemente* parecen coincidir con las del responsable y encargado de tratamiento.

El artículo 14 del proyecto, *Gestión de los riesgos*, dispone:

“El Responsable del Servicio es el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.”

“Los Responsables de Seguridad, dentro de su ámbito de actuación, son los encargados de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.”

“Los Responsables de la Información y del Servicio son quienes gestionan y asumen los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.”

Los Responsables de la Información y los Responsables del servicio se encuentran regulados en el artículo 10 del proyecto, que previene que coincidirán en una misma figura las responsabilidades de la Información y del Servicio salvo en aquellos casos en los que éste maneje información de diferentes unidades o cuando la prestación del servicio no dependa de la unidad responsable de la información.

Los Responsables de la Información y del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos de seguridad de la información que manejan y de los servicios bajo su competencia y, por tanto, de su protección.

Los Responsables de la Información tendrán como competencia participar, y en su caso, aceptar los riesgos residuales que afecten a los activos de información bajo su ámbito de actuación, incluyendo aquellos que afecten a datos de carácter personal.

Por su parte, los Responsables del Servicio, tendrán la competencia de determinar los niveles de seguridad requeridos para el servicio o servicios bajo su ámbito de actuación, estableciendo los requisitos y valoración en términos de criticidad y disponibilidad. Tendrán también la competencia de participar, y en su caso, aceptar los riesgos residuales que afecten a los servicios bajo su ámbito de actuación.

El precepto -artículo 10 de la Orden proyectada- dispone que, si los servicios y la información manejada incluyen datos de carácter personal, los Responsables de la Información y los Responsables del Servicio deberán tener en cuenta, además, los requisitos derivados de la legislación correspondiente sobre protección de datos.

Con el propósito de no confundir las funciones del responsable y encargado de tratamiento (artículo 12) de una parte y de otra las de los Responsables de la Información y del Servicio (artículos 14 y 10) y concretar los límites que los separan se trae a colación el Informe de este Servicio Jurídico 170/2018 que detalla 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.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país

de destino estuviere protegido por salvaguardas adecuadas a las previstas en la propia directiva”.

Y en este mismo sentido se pronuncia el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que tiene por objeto “proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales” (artículo 1.2.), destacando en su Considerando 1 que “la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental” y en su Considerando 10 que “para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo”.

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento” y “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para “asesorar

sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento” (artículo 57.1.c) RGPD)”.

VI

Respecto a la figura del delegado de protección de datos (DPD) regulada en los artículos 37 a 39 del RGPD, se observa que el proyecto informado no contempla al DPD como uno de los sujetos de la estructura organizativa que tiene encomendada la gestión de la seguridad de la información en su ámbito de aplicación (descrita en su artículo 7). Tampoco dedica a su regulación un precepto específico.

No obstante, las menciones que el proyecto hace en su articulado al DPD son plenamente acordes con la concepción que el RGPD tiene de esta figura y con las funciones esenciales que le encomienda.

El artículo 38 del RGPD dispone 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.”*

Por su parte, el artículo 39 del RGPD indica que *“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 este sentido, el documento de directrices sobre los delegados de protección de datos, adoptado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE y revisado el 5 de abril de 2017 (documento WP243), aclara que *“El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar*

«medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (artículo 24, apartado 1). El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD».

El proyecto de Orden se refiere al DPD con ocasión de regular la gestión de los riesgos. Así, el **artículo 6.b) 1** del proyecto versa sobre el análisis y gestión de los riesgos y hace una referencia expresa al 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.

Como se ha indicado, el proyecto de Orden no incluye al DPD en la relación de sujetos que integran su estructura organizativa. No obstante, le otorga la condición de vocal del Comité de Seguridad de la Información (CSI), con voz, pero sin voto lo que resulta plenamente respetuoso con el RGPD pues permite salvaguardar la independencia del DPD al tiempo que le permite desempeñar su función asesora.

El **artículo 8** del proyecto, bajo la rúbrica Comité de Seguridad de la Información (CSI), *Composición y funciones del Comité de seguridad de la información*, dice que, de acuerdo al artículo 13 del ENS, estará compuesto por varios vocales siendo uno de ellos *“La persona designada como Delegado de Protección de Datos del Departamento, que actuará como asesor con voz, pero sin voto, para garantizar su independencia en atención a la naturaleza de sus funciones de asistencia y apoyo.”*

También hacen mención a las funciones del DPD los **artículo 14 y 16** del proyecto normativo, en ambos casos, en línea con lo previsto en el RGPD. Así, cabe decir que el **artículo 14** del proyecto de Orden, bajo el título *“Gestión de los riesgos”*, indica en su párrafo último:

“En el caso de que existan tratamientos de datos personales, se deberá tener en cuenta lo dispuesto en el artículo 16, de modo que los requisitos identificados conforme a dicho artículo y, con el asesoramiento específico del Delegado de Protección de Datos, se puedan añadir a los establecidos conforme al Real Decreto 311/2022, de 3 de mayo, si así fuera necesario, en particular, fijando el nivel de seguridad a un nivel más alto. En estos casos, si el resultado del análisis es que los tratamientos de datos personales fuesen de alto riesgo, estos requisitos se elaborarán con la formalidad de una evaluación de impacto en la protección de datos, conforme al artículo 35 del RGPD y los criterios establecidos por la Agencia Española de Protección de Datos (AEPD). En este aspecto, también se deberá tener en cuenta la regulación de la seguridad de los tratamientos de datos personales, especificada en el artículo 32 del RGPD.

Por su parte, el **artículo 16** de la Orden establece que *“Deberá comunicarse al Delegado de Protección de Datos del Departamento los incidentes de seguridad que puedan suponer una violación de la seguridad de los datos personales.”*

En consideración a lo expuesto, teniendo en cuenta la regulación que el RGPD hace de la figura del DPD, esta Agencia aprecia que las previsiones normativas sobre el DPD del proyecto de Orden (artículos 6.1.b; 14 y 16) se adecuan a la normativa de protección de datos de carácter personal.

No obstante, **sería aconsejable que la Orden incorporase las previsiones del artículo 37.5 del RGPD sobre la designación del DPD**, máxime cuando en el ámbito de esta PSI es preceptivo su nombramiento de acuerdo con el artículo 37.1.a) del RGPD. Debería hacerse constar que el delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 (artículo 37.5 del RGPD).

Igualmente, **sería aconsejable incorporar el artículo 38.3 del RGPD** que concreta la “Posición del delegado de protección de datos” al disponer:

“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 6** del proyecto, “*Requisitos de Seguridad de la Información*”, hace referencia en su **apartado “s)”** al “*Uso de Herramientas de Inteligencia Artificial Generativa Externa*”, en los términos siguientes:

“El MPTMD adoptará el principio de prudencia y control estricto sobre el uso de tecnologías y servicios externos, especialmente aquellos emergentes como la Inteligencia Artificial (IA) generativa. En aplicación de este principio, y para salvaguardar la confidencialidad, integridad y disponibilidad de la información bajo su responsabilidad, no se permitirá la transferencia o uso de información del organismo en plataformas de IA generativa externas que no hayan sido explícitamente evaluadas y autorizadas por los órganos competentes. Este enfoque se alinea con las exigencias de las normativas de protección de datos y el marco regulatorio europeo sobre Inteligencia Artificial (Reglamento (UE) 2024/1689), promoviendo un uso seguro y ético de la tecnología.”

Es obligado indicar, a propósito del precepto transcrito, que cuando una organización utiliza IA generativa puede estar efectuando un tratamiento de datos personales de múltiples formas. Esta tecnología puede generar, transformar o reproducir información basada en grandes volúmenes de datos, muchos de ellos personales. Los datos que se usen para entrenar modelos pueden ser identificables o reidentificables. También la aplicación de modelos sobre la información puede generar resultados que afecten a personas concretas.

Así pues, cuando el **artículo 6.s)** del proyecto alude a la posibilidad de que el MPTMD permita (previa evaluación y autorización por los órganos competentes) “la transferencia o uso de información del organismo en plataformas de IA generativa

externas”, no puede ignorar que, si tal información permite identificar directa o indirectamente a una persona física, tiene la naturaleza de dato personal (ex artículo 4.1 del RGPD).

Por consiguiente, **la transferencia de información prevista en la norma proyectada implicaría un tratamiento de datos personales (su comunicación a terceros) que únicamente podría llevarse a cabo si cumpliera con la normativa de protección de datos: que el tratamiento tuviera una base jurídica adecuada conforme al artículo 6.1. del RGPD; que el responsable hubiera cumplido la obligación de informar de ese tratamiento al interesado (artículos 13 o 14 del RGPD); que hubiera adoptado las medidas para garantizar la aplicación efectiva de los principios de protección de datos y la seguridad del tratamiento, la evaluación de impacto y la atención a las solicitudes de derechos del titular de los datos.**

De manera que, debemos recordar que, **en caso de uso de IA generativa el MPTMD tiene la obligación de examinar si existe un tratamiento de datos de carácter personal y en caso afirmativo verificar que cumple estrictamente con la normativa de protección de datos de carácter personal.**

Por otra parte, es preciso centrarse en las disposiciones de los **artículos 6,I) y 16, penúltimo párrafo**, del proyecto informado que prevén la existencia de tratamientos de datos personales que pueden realizarse como consecuencia de la implantación de medidas de seguridad que tengan un objetivo distinto de la protección de datos personales.

El artículo 6, I), “*Registro de actividad*”, dispone:

“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.”

Esta disposición es una copia fiel del artículo 24.1 del ENS sobre el “registro de actividad”. Los registros de la actividad de las personas usuarias cuya creación habilita el precepto 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*) respetando en estos casos, entre otras, la normativa de protección de datos de carácter personal. Por tanto, **esta disposición -artículo 6,I)- se informa favorablemente.**

El último párrafo del artículo 16 del proyecto de Orden -“*Protección de Datos de Carácter Personal*”- dispone:

“Los servicios de ciberseguridad y administración de sistemas, dependientes de los respectivos Responsables de los Sistemas, podrán implementar

tratamientos de datos personales como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto de la protección de datos personales, en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022, de 3 de mayo, y teniendo en cuenta, entre otros, los principios de limitación de finalidad; prohibición del tratamiento de los datos personales para fines distintos; el 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.”

Llegados a este punto es obligado referirse al artículo 24 del ENS -“Registro de actividad y detección de código dañino”- cuya versión actual se introdujo por el RD 311/2022 que incorporó a su redacción final las observaciones del Informe 64/2021 del Servicio Jurídico de esta Agencia al Proyecto de Real Decreto que aprobaba el Esquema Nacional de Seguridad. El precepto 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 artículo 24.2 del ENS permite que se efectúe un tratamiento de datos que consistirá en “analizar las comunicaciones entrantes o salientes” y que se realizará “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”. De modo que, con esa finalidad, el tratamiento efectuado permita (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.

El tratamiento así definido solo se podrá llevar a cabo “en la medida estrictamente necesaria y proporcionada”. El precepto del ENS exige expresamente 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 tal finalidad.

Además, el artículo 24.2 del ENS exige también que el tratamiento al que se refiere se adecúe a los principios de limitación de la finalidad, minimización de datos y limitación del plazo de conservación y que se observe el RGPD. Por otra parte, el artículo 24.2 del ENS identifica quiénes pueden efectuar el tratamiento así definido: los sujetos que se mencionan en su artículo 2, que remite al sector público en los términos previstos en el artículo 2 de la Ley 40/2015 (apartado 1) y (apartado 2) a los sistemas que traten información clasificada.

La redacción actual del artículo 24.2 del ENS, en particular, la exigencia de que el tratamiento sea estrictamente “necesario” y “proporcionado” a la finalidad a la que busca atender y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación se introdujo al incorporar las observaciones del Informe del Servicio Jurídico de esta Agencia (Informe 64/2021)

Sin embargo, el artículo 16 del proyecto ha omitido mencionar que el tratamiento descrito deberá ser estrictamente necesario y proporcionado a la finalidad perseguida. Tampoco concreta en qué consistirá el tratamiento (lo que sí hace el artículo 24.2 del ENS, que precisa que consistirá en “analizar las comunicaciones entrantes o salientes” y que se realizará “para una finalidad específica”: “la seguridad de la información”). El proyecto en su artículo 16 se limita a hacer una remisión genérica al artículo 24.2 del ENS (“en base a lo dispuesto en el artículo 24 del Real Decreto 311/2022”).

Esta Agencia entiende que la actual redacción del artículo 16, penúltimo párrafo, del proyecto informado debe rechazarse por las razones indicadas.

Traemos a colación el Informe precitado, 64/2021, del que se reproducen algunos párrafos. El Informe, con ocasión de valorar la redacción del artículo 24.2 del ENS, expuso las razones por las que esa norma debía incluir una mención expresa a la proporcionalidad del tratamiento previsto. Argumentos que resultan aplicables al presente caso y son motivo suficiente para exigir que el artículo 16 del proyecto de Orden subsane la omisión en la que incurre e incorpore la exigencia de que el tratamiento previsto en esa norma sea el “**estrictamente proporcional y necesario**” para la finalidad que persigue, garantizar la seguridad de la información.

“[...] 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.

[...]

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)."

El Informe 64/2021, tras indicar que el texto del artículo 24 del RD debía recoger una referencia expresa a los principios mencionados, propuso una redacción alternativa que es la del actual artículo 24.2 del ENS.

El informe precitado destacó, además, la necesidad de incluir en el precepto (artículo 24 del ENS) o en los Anexos garantías adicionales: el principio de limitación de la finalidad, minimización y limitación del plazo de conservación:

"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."

Como se ha indicado en los párrafos precedentes esta Agencia estima **que debe rechazarse la actual redacción del artículo 16** del proyecto de Orden no solo por la importante **omisión acerca del carácter estrictamente proporcional y necesario del tratamiento** en relación con la finalidad a la que atiende. También debe rechazarse toda vez que el artículo 16 mencionado **no explicita en qué consiste el tratamiento y su finalidad**, limitándose en su lugar a hacer una remisión a los términos del artículo 24 del ENS. Se reitera por ello que **resulta necesario que el precepto contenga una descripción del tratamiento que habilita a efectuar y de su finalidad** que deberán ser acordes con la previsión del artículo 24.2 del ENS, pudiendo consistir en cualquier caso en una copia fiel del texto del precitado artículo del ENS.

VIII

En conclusión, este Informe **valora positivamente el artículo 5** de la Orden proyectada, *"Principios de la seguridad de la información"*, y lo considera correcto y coherente con la normativa de protección de datos

En tal sentido ha destacado que el apartado b) del artículo 5 del proyecto obliga a que todos los tratamiento de datos personales que se efectúen en su marco de aplicación sean objeto de un análisis de riesgos; incorpora una previsión temporal sobre cuándo deberán realizarse (apartado d) del artículo 5) y el artículo 5, apartado a) recoge la obligación que impone el artículo 32 del RGPD al responsable y al encargado del tratamiento de aplicar *“medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”*.

Sobre el **artículo 6** del proyecto, *“Requisitos de la seguridad de la información”*, y en particular respecto al requisito del *“análisis y gestión de los riesgos”* (artículo 12.b, del ENS) , la Orden proyectada **acoge una visión conjunta e integrada de tal gestión** en relación con los sistemas de información que traten datos de carácter personal. Se informa por ello favorablemente ese precepto con la salvedad de sus apartados “l” y “s”, que han sido objeto de una análisis por separado.

Asimismo, se **informa favorablemente** la regulación que el proyecto de Orden hace en sus artículos 6 b, punto 2, 14 y 16 en sus tres primeros párrafos, de la prevalencia que debe darse, respecto a las previstas en el ENS, a las **medidas de seguridad agravadas** que resulten de haber efectuado un análisis de riesgos y en su caso una evaluación de impacto.

En cuanto al **responsable** y al **encargado del tratamiento**, la concepción de estas figuras y las funciones que tienen encomendadas en el proyecto de Orden (artículos 12 y 6.1.b) se ajusta a las previsiones del RGPD.

Sobre el **DPD**, el Informe valora favorablemente la regulación del proyecto, que se adecua al RGPD tanto en la concepción de esta figura como en las funciones esenciales que le atribuye. No obstante, el Informe **aconseja incluir referencias expresas a los artículos 37.5 del RGPD**, relativo a su designación y las condiciones que debe reunir, y **38.3. del RGPD**, relativo a la “Posición del delegado de protección de datos”.

Respecto al *“Uso de Herramientas de Inteligencia Artificial Generativa Externa”* prevista en el artículo **6.1.s** del proyecto, el Informe **recuerda** que, en caso de uso de IA generativa el MPTMD tiene **la obligación de examinar si existe un tratamiento de datos de carácter personal** y, en caso afirmativo, verificar que cumple estrictamente con la normativa de protección de datos de carácter personal.

En relación a los tratamientos de datos personales que se realicen como consecuencia de la implantación de medidas de seguridad que tengan un objeto distinto de la protección de datos -artículo 16, penúltimo párrafo del proyecto- consideramos que **debe rechazarse la actual redacción por la importante omisión de la que adolece**, habida cuenta de que ni incluye la exigencia de que el tratamiento sea estrictamente proporcional y necesario en relación con la finalidad a la que atiende, ni ha explicitado en qué consiste el tratamiento ni su finalidad, limitándose a hacer una remisión a los términos del artículo 24 del ENS.