I

Dicho documento, fechado el 5 de septiembre de 2018 y carente de firma, plantea la inexistencia de inconvenientes en el ordenamiento vigente que impidan que la figura del delegado de protección de datos (DPD) y el responsable de seguridad del ENS (RSEG), recaigan en la misma persona física u órgano colegiado, cuando se satisfagan los requisitos de capacidad, experiencia e **independencia** recogidos en ambas regulaciones.

El informe plantea varios argumentos con relación al planteamiento inicial:

1. *Que el RSEG se define en el ENS (Art. 10 con una responsabilidad claramente diferenciada del resto de los elementos responsables: Responsable de la Información (RINF), de los Servicios (RSER) y del Sistema (RSIS).*

En esta línea se plantea la necesidad de establecer independencia y segregación de funciones entre los perfiles indicados en los siguientes términos:

- *El RINF determina los requisitos de la información tratada.*
- *El RSER determina los requisitos de los servicios prestados.*
- *El RSEG determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios que han sido definidos previamente por el RINF y el RSER.*
- *La actuación del RSEG es absolutamente independiente (no está condicionada por el RSIS.*

2. *El Considerando (77) del RGPD señala que:*

   "Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza y probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité

> *también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas e indicar qué medidas pueden ser suficientes en casos para afrontar el riesgo en cuestión."*

Señala dicho informe que precisamente el RSEG tiene la función de proporcionar estas indicaciones de seguridad a las que refiere el considerando 77, y que a opinión de la AEPD expresada en el documento titulado "EL DELEGADO DE PROTECCIÓN DE DATOS EN LAS ADMINISTRACIONES PÚBLICAS" es contraria cuando en el mismo se señala:

> *"Si este es el caso, debe tenerse en cuenta la necesidad de evitar conflictos de intereses entre las diversas ocupaciones. El DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC o responsables de seguridad de la información."*

Igualmente, el informe pone de manifiesto que existe una colisión con lo previsto en el artículo 35 del RGPD, que señala que *"2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto a la protección de datos."*

Se da a entender en dicho párrafo que necesariamente este asesoramiento en las evaluaciones de impacto se corresponde con acciones relacionadas con *"el modo en el que van a ser tratados los datos"*.

3. *La posibilidad de integrar las funciones del DPD con las del RSEG no parece encontrar oposición tampoco en lo señalado en las "Directrices sobre los Delegados de Protección de Datos" (revisión del 5.4.2017) del Grupo de Trabajo sobre Protección de Datos del Artículo 29, asumidas por el Comité Europeo de Protección de Datos cuando señala, entre otros los siguientes extremos:*

   - *[Epígrafe 1 "Introducción", párrafo quinto]: "Además de facilitar el cumplimiento mediante la aplicación de instrumentos de rendición de cuentas (tales como facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos los DPD actúan como intermediarios entre las partes interesadas correspondientes (P. ej. Autoridades de control, interesados y unidades de negocio dentro de la organización)."*

Dicho informe manifiesta que esta afirmación hace coincidente la posición del RSEG con la posición del DPD.

- *[Epígrafe 1 "Introducción", párrafo sexto]: "Los DPD no son personalmente responsables en caso de incumplimiento del RGPD… El cumplimiento de las normas sobre protección de datos es responsabilidad del responsable o del encargado del tratamiento".*

Igualmente, manifiesta dicho informe que esto hace coincidente el papel del DPD con el RSEG.

- *[Epígrafe 3.5 "Conflicto de intereses"]: "el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización esto deberá considerarse caso por caso."*

Con relación a es epígrafe el informe pone de manifiesto nuevamente que la posición del RSEG y del DPD son coincidentes.

- *[Epígrafe 4.2 "Papel del DPD en una evaluación de impacto relativa a la protección de datos, párrafo segundo]: "El Grupo de Trabajo del artículo 29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones, entre otras (como mínimo): si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos / qué metodología debe seguirse al llevar a cabo una evaluación de impacto / si debe realizarse la evaluación de impacto en la propia organización o subcontratar / qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos de los interesados / si la evaluación de impacto a la protección de datos se ha llevado a cabo correctamente o no y si sus concusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD."*

Asume el informe que dicho papel en las evaluaciones de impacto es coincidente para ambas figuras; el RSEG y el DPD.

- *[Epígrafe 4.4 "Enfoque basado en el riesgo" párrafo primero]: "El artículo 39, apartado2, requiere que el DPD desempeñe sus funciones "prestando la debida atención a los riesgos asociados o*

las operaciones de tratamiento teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento".

Considera también el informe que el mero enfoque de riesgos tanto para las actividades de la seguridad como para las actividades de los tratamientos de datos debe entenderse como una coincidencia más de la figura del RSEG con la figura del DPD.

4. *Las funciones que el art. 39 del RGPD otorga al DPD, en lo relativo a su relación con el Responsable o el Encargado del Tratamiento, tienen su correlato en el ENS respecto de las funciones del RSEG en su relación con los RINF y RSER, lo que ayuda a hermanar ambas figuras.*

II

Con carácter previo a analizar la concreta cuestión que planteada en la consulta este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan. En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados "Tecnologías de la Información y las Comunicaciones (TIC)"), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, cuyo Preámbulo señala que *"la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones*

necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios" añadiendo que *"en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles".*

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 *"no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos".*

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la

Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

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

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

en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva".

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

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

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito

mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las "autoridades de control", funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para *"asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento"* (artículo 57.1.c) RGPD).

III

Entrando ya a analizar la cuestión planteada en la consulta y relativa a la compatibilidad funcional del "delegado de protección de datos del RGPD" y el "responsable de seguridad del Esquema Nacional de Seguridad", resulta necesario analizar las funciones de cada una de estas figuras según su normativa específica y la posible existencia de un conflicto de intereses que impidiese dicho nombramiento.

En cuanto al delegado de protección de datos se trata de una figura que adquiere una importancia esencial en el nuevo modelo de protección establecido en el RGPD, asumiendo la función de asesorar y supervisar las actividades de tratamiento de los responsables o encargados y cuyo nombramiento podrá tener carácter obligatorio o voluntario, según los casos. El RGPD lo regula en la Sección 4 del Capítulo IV, artículos 37 a 39, regulación que deberá completarse, una vez que entre en vigor, con lo dispuesto en el Capítulo III del Título III, artículos 34 a 37, del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (PLOPDPGDD), actualmente en tramitación en el Senado.

Por lo que se refiere a sus funciones, el artículo 39 RGPD establece las siguientes:

"1.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."

Asimismo, el Proyecto de Ley Orgánica prevé en su artículo 36 que el delegado pueda inspeccionar los procedimientos y emitir recomendaciones, y en el artículo 37, dentro de las funciones de supervisión y asesoramiento del delegado de protección de datos atribuidas por el artículo 39 del Reglamento general de protección de datos, la posibilidad de que el mismo pueda atender las reclamaciones que le planteasen los afectados con carácter previo a que éstos acudan a la autoridad de protección de datos. Igualmente, se prevé la posibilidad de que planteada una reclamación ante dicha autoridad ésta pueda consultar al delegado de protección de datos acerca de la misma con carácter previo a la tramitación de la reclamación.

En cuanto a la designación del delegado de protección de datos, el artículo 37 RGPD establece los supuestos en que la misma será obligatoria para responsables y encargados del tratamiento, y en cuanto a la capacitación,

señala en su apartado 5 que *"será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39"*, añadiendo el artículo 35 PLOPDPGDD que el cumplimiento de dichos requisitos *"podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos"*.

Asimismo, el artículo 37.5 RGPD prevé que *"el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios"* y el artículo 38.3, al regular la posición del delegado de protección de datos, subraya su independencia al señalar que *"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"* y su apartado 6 añade que *"el delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses"*. En este mismo sentido, el artículo 36.2 del PLOPDPGDD especifica que *"cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses".*

Precisamente, en relación con el posible conflicto de intereses, las directrices sobre los delegados de protección de datos adoptadas por el Grupo de Trabajo sobre Protección de Datos del Artículo 29, revisadas por última vez y adoptadas el 5 de abril de 2017, señalan lo siguiente:

3.5. Conflicto de intereses

El artículo 38, apartado 6, permite a los DPD «desempeñar otras funciones y cometidos». No obstante, requiere que la organización garantice que «dichas funciones y cometidos no den lugar a conflicto de intereses».

La ausencia de conflicto de intereses está estrechamente ligada al requisito de actuar de manera independiente. Aunque los DPD puedan tener otras funciones, solamente podrán confiárseles otras tareas y cometidos si estas no dan lugar a conflictos de intereses. Esto supone, en especial, que el DPD no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales. Debido a la estructura organizativa específica de cada organización, esto deberá considerarse caso por caso.

Como norma general, los cargos en conflicto dentro de una organización pueden incluir los puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI) pero también otros cargos inferiores en la estructura organizativa si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento. Asimismo, también puede surgir un conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o al encargado del tratamiento ante los tribunales en casos relacionados con la protección de datos.

Dependiendo de las actividades, tamaño y estructura de la organización, puede ser una práctica recomendable que los responsables y encargados del tratamiento:

determinen los puestos que podrían ser incompatibles con la función de DPD;

elaboren normas internas a tal efecto con el fin de evitar conflictos de intereses;

incluyan una explicación más general sobre los conflictos de intereses;

declaren que su DPD no tiene ningún conflicto de intereses con respecto a sus funciones como DPD, como medio de concienciar sobre este requisito;

incluyan salvaguardias en las normas internas de la organización y garanticen que el anuncio de convocatoria para el puesto de DPD o el contrato de servicios sea lo suficientemente preciso y detallado para evitar un conflicto de intereses. En este contexto, debe tenerse en cuenta también que los conflictos de intereses pueden adoptar diversas formas en función de si el DPD se contrata interna o externamente.

Por otro lado, el documento elaborado por la Agencia Española de Protección de Datos sobre el "El delegado de protección de datos en las Administraciones Públicas" añade lo siguiente:

El RGPD prevé que el DPD podrá desarrollar su actividad a tiempo completo o a tiempo parcial y también que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. En órganos, organismos o entes de gran tamaño en que exista un único DPD lo habitual será que desempeñe sus funciones a tiempo completo. Es, incluso, posible que el DPD formalmente nombrado esté respaldado por una unidad específicamente dedicada a la protección de datos. En entidades de menor tamaño será posible que el DPD compagine sus funciones con otras. Si éste es el caso, debe tenerse en cuenta la necesidad de evitar conflictos de intereses entre las diversas ocupaciones. El DPD actúa como asesor y supervisor interno, por lo que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos (p.ej.: responsables de ITC, o responsables de seguridad de la información).

En cuanto al responsable de la seguridad de la información, 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, lo regula en su artículo 10:

"Artículo 10. La seguridad como función diferenciada.

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."

Partiendo de dicho artículo, el documento titulado <<Análisis jurídico de la compatibilidad funcional del "delegado de protección de datos del RGPD" y el

responsable de seguridad del Esquema Nacional de Seguridad”>> considera que no existe un conflicto de intereses por las detalladas razones que se han expuesto anteriormente y que pueden resumirse en las siguientes:

1.- El responsable de seguridad tiene una responsabilidad claramente diferenciada del resto de los elementos responsables, siendo su función la de señalar las medidas de seguridad que puedan satisfacer los requisitos señalados por los responsables de la información y de los servicios y actuando con plena independencia respecto del responsable del sistema.

2.- Al responsable de seguridad le corresponde una serie de funciones, como la de proporcionar las indicaciones de seguridad, facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos o la de actuar de intermediario con las partes interesadas que se corresponderían con las funciones que el RGPD atribuye al delegado de protección de datos.

Por todo ello, el citado documento concluye:

“Por tanto, a nuestro modo de ver, el problema se reduce a garantizar, en cada entidad del ámbito de aplicación del ENS y en cada caso, que, muy especialmente, entre el RSEG y el RSIS existe la debida independencia.

Si esta garantía (que entendemos está recogida en el ENS) quedara igualmente expresada en la Política de Seguridad de la organización de que se trate, entendemos que no habría impedimento para que ambas figuras, DPD y RSEG, puedan recaer sobre la misma persona u órgano colegiado, habiendo sido satisfechas, obviamente, los requisitos adicionales de capacidad, formación y experiencia recogidos en el RGPD.”

IV

Sin embargo, y partiendo necesariamente de la diferenciación existente entre seguridad de la información y protección de datos de carácter personal apuntada anteriormente, este Gabinete Jurídico no comparte dicha conclusión por las siguientes razones:

1.- En cuanto a la segregación de funciones a la que refiere el punto primero del referido informe, recogida en el artículo 10 del ENS, sería también extensible a la figura del DPD ya que así lo prevé el RGPD en su artículo 38.3:

"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".

A diferencia de las figuras que define el artículo 10 del ENS, que reciben órdenes del responsable de la información, el DPD no puede recibir instrucciones de ninguna de las figuras ya mencionadas y obrará con total independencia de las mismas. Cuestión que, lógicamente, impide que las funciones del DPD puedan ser llevadas a cabo por parte de cualquiera de los roles implicados en el cumplimiento del ENS quienes pueden recibir instrucciones del responsable de la información. Podemos decir, que el principio de independencia del DPD tiene un ámbito más restrictivo que el que tiene el RSEG en el ámbito del ENS.

2.- Con relación al segundo punto del informe y, en consonancia con lo anterior, el DPD informa y asesora al responsable, supervisa el cumplimiento, lleva a cabo labores de concienciación y formación del personal implicado en los tratamientos de datos personales y coopera con la autoridad de control con independencia del resto de las figuras implicadas en la seguridad de la información de las Administraciones Públicas.

El papel del RSEG es garantizar la seguridad de la información de las Administraciones Públicas mientras que el papel del DPD puede resumirse en garantizar los derechos y libertades de las personas cuyos datos son tratados con independencia rindiendo cuentas directamente al más alto nivel jerárquico del responsable o del encargado del tratamiento. Se trata, por lo tanto, de funciones de asesoramiento distintas en sus principios y en su alcance, motivo por el cual dichas funciones responden a ordenamientos diferenciados.

En consecuencia, el RSEG proporciona directrices encaminadas a garantizar la seguridad de la información, sean datos personales o simplemente información

de las Administraciones Públicas, mientras que las directrices que debe proporcionar el DPD (considerando 77) están encaminadas a garantizar los derechos y libertades de las personas y no la seguridad de la información. A diferencia del RSEG, quien puede recibir instrucciones del RINF, el DPD no debería recibir instrucciones en el desempeño de sus funciones.

El nombramiento del DPD sobre la misma persona o entidad que ostenta la condición de RSEG supondría, negar el principio de independencia y segregación de funciones del ENS (art. 10) y, una negación del principio de independencia que determina el RGPD (Art. 38.3).

Con respecto al asesoramiento del DPD al responsable en las evaluaciones de impacto, dicho asesoramiento, no puede interpretarse como una manera en la que el DPD reciba instrucciones del responsable o que participe en la toma de decisiones sobre los tratamientos. El asesoramiento del DPD con relación al responsable del tratamiento debe de entenderse de la siguiente forma:

- El DPD asesora al responsable, tanto en las evaluaciones de impacto como en cualquier aspecto de las actividades de tratamiento que lleve a cabo.
- El responsable toma decisiones atendiendo, o no, al asesoramiento del DPD, pues es el responsable finalmente quien determina los fines y medios y quien asumirá las posibles consecuencias que para, los derechos y libertades de las personas, pudieran tener los tratamientos que lleva a cabo.

Por lo tanto, corresponde únicamente y en última instancia, al responsable decidir el modo en que van a ser tratados los datos. El DPD asesora pero no decide sobre dicho modo en el que los datos van a ser tratados y mucho menos correspondería al RSEG llevar a cabo dicho asesoramiento pues, su ámbito de actuación, se centra en garantizar la seguridad de la información.

3.- Con relación a las conclusiones que se expresan en el punto tercero del argumentario de dicho informe, concretamente a la afirmación de que facilitar o llevar a cabo evaluaciones de impacto y auditorías de protección de datos por parte del DPD o actuar como intermediario entre las partes interesadas (autoridades de control, interesados y unidades de negocio dentro de la

organización) señalar que se trata, como ya se ha indicado, de ámbitos de actuación distintos con objetivos que deben ser diferenciados. Concretamente el RSEG actúa con el fin de garantizar la seguridad de la información y las funciones del DPD deben encaminarse a garantizar los derechos y libertades de las personas en los tratamientos que lleva a cabo el responsable.

Igualmente carece de sentido la consideración de equiparar la posición del RSEG y del DPD por el mero hecho de que ninguno de los dos sea responsable de la información o responsable del tratamiento y, en caso de incumplimiento normativo, ninguno de los dos deba asumir las responsabilidades de dicho incumplimiento, tal afirmación equivaldría a asumir que cualquier persona que no sea el responsable podría asumir el rol del DPD o el de RSEG. Como ya se ha indicado, corresponde al responsable en caso de incumplimiento asumir las posibles consecuencias del mismo pero el hecho de que el tanto la figura del RSEG como el DPD no asuman esta responsabilidad, en ningún caso, no puede entenderse como una equiparación de roles o funciones.

Tampoco tendría de sentido equiparar el rol y posición del RSEG y del DPD por el simple hecho de que ninguno de los dos pueda ocupar cargo en la organización que le lleve a determinar los fines y medidas del tratamiento de datos personales. Que ambos estén sujetos a este principio de independencia no implica que ambos actúen con los mismos objetivos, cabría señalar nuevamente que el RSEG tiene un ámbito de actuación diferenciado del ámbito de actuación del DPD, el primero debe garantizar la seguridad de la información mientras que el segundo debe garantizar los derechos y libertades de las personas cuyos datos son tratados.

Sería un error considerar que las actividades de análisis de riesgos necesarias para llevar a cabo en las evaluaciones de impacto en protección de datos personales son coincidentes con las actividades de análisis de riesgos realizadas para determinar las medias de seguridad para paliar los riesgos de para la seguridad de la información. Las evaluaciones de impacto en protección de datos están encaminadas a determinar los riesgos de un tratamiento para los derechos y libertades de las personas y es una actividad diferenciada de la que se precisa para llevar a cabo el análisis de riesgos para la seguridad de la información con relación a los riesgos de las tecnologías de la información y las comunicaciones.

La coincidencia del enfoque de riesgos del ENS con el RGPD no puede utilizarse para poner de manifiesto la identidad de roles y funciones del RSEG con el DPD. El análisis de riesgos tiene diferentes finalidades, como ya se ha mencionado, en el ENS tiene por objeto determinar los riesgos para la información de las Administraciones Públicas mientras que en el RGPD tiene por finalidad determinar los riesgos que los tratamientos de datos personales implican para los derechos y libertades de las personas.

4.- Con relación a lo que se pone de manifiesto en el punto cuarto del argumentario, carece de sentido el “hermanamiento” de ambas figuras ya que equivaldría a manifestar que en ningún caso existiría un posible conflicto de intereses, o que existiera riesgos para la independencia del DPD tal y como expresa el artículo 38.3 del RGPD.

En este sentido hay que recordar que ya el propio Centro Criptológico Nacional y en relación con el responsable de seguridad de la LOPD, con funciones más limitadas que el actual DPD del RGPD (persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables) y que carecía del estatus de independencia del que goza el DPD, estimaba conveniente separar ambas figuras (https://administracionelectronica.gob.es/dam/jcr:25a902cd-1769-4c1d-8da7-4a26b3109174/Esquema_Nacional_de_Seguridad_-Preguntas_frecuentes.pdf)

> 4.5. ¿El Responsable de Seguridad del ENS puede ser la misma persona que el Responsable de Seguridad de la LOPD?
>
> Formalmente nada lo impide. Debemos hacer constar que ambos perfiles requieren una formación muy específica y diferenciada. (Por ejemplo, el Responsable de Seguridad ENS es un perfil eminentemente tecnológico, mientras que el responsable de seguridad LOPD debe poseer, además, el conocimiento jurídico pertinente). Por tanto, dándose la circunstancia de que la persona designada goce de la formación adecuada en ambas responsabilidades, no existe inconveniente.
>
> Independientemente de lo anterior, sobre todo en organizaciones de tamaño significativo, debe entenderse como más conveniente que ambos responsables (en caso de personas físicas) sean distintos, pudiendo formar parte, eso sí, de un Comité de Seguridad de amplio espectro y cuyo titular será el Responsable formal de ambas funciones.

Finalmente, cabe señalar la consideración incluida en la norma ISO/IEC 29151:2017 Information technology – Security techniques - Code of practice for

personally identifiable information protection en la que, con respecto a la necesidad de establecer la debida segregación de funciones, se incluye la siguiente previsión: "*Duties and area of responsibilities for personally identifiable information (PII) protection should be independent of those for information security. While recognizing the importance of information security for the protection of PII, it is important that duties and area or responsibilities of the security and PII protection be as independent of each other as possible. If necessary or helpful, in the interest of PII protection, coordination and cooperation of those responsible for information security and for PII protection should be facilitated*".

V

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

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

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

que podrían afectar a los derechos y libertades de las personas o incluso a la propia seguridad de la información.

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

Así lo han entendido en organizaciones con importantes responsabilidades en materia de seguridad de la información. En este sentido, en el Ministerio de Defensa, en el que la información "constituye un recurso estratégico del Departamento sobre el que se debe buscar la superioridad para facilitar el cumplimiento y alcanzar el éxito de los cometidos encomendados al Ministerio de Defensa y de las misiones de las Fuerzas Armadas" (artículo 2 de la Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa), está dotado de una estructura que depende del Secretario de Estado de Defensa en cuanto órgano responsable de la dirección, impulso y gestión de las políticas de las tecnologías, sistemas y seguridad de la información (artículo 4 del Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa) y que se desarrolla en diferentes órdenes ministeriales, además de la ya citada Orden DEF/1196/2017: la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa y la Orden ministerial 5/2017, de 9 de febrero por la que se aprueba la Política de Gestión de Documentos electrónicos del Ministerio de Defensa.

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

En conclusión, es criterio de este Gabinete Jurídico que debe existir la necesaria separación entre el delgado de protección de datos regulado en el

RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.