

Ref.: Delegada de Protección de Datos

## INFORME

### INFORME DE LA DELEGADA DE PROTECCIÓN DE DATOS DE LA CONSEJERÍA DE DERECHOS SOCIALES, IGUALDAD, DIVERSIDAD Y JUVENTUD, SOBRE EL PROYECTO DE ORDEN DE LA CONSEJERA POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN ESTE DEPARTAMENTO EN EL ÁMBITO DE LA ADMINISTRACIÓN ELECTRÓNICA.

Recibida petición de informe por parte de la Secretaria General Técnica de este Departamento, mediante comunicación de régimen interno con registro de salida DIDJ/21376/2022, de 11 de julio de 2022, remitiendo el informe de la Dirección General de Telecomunicaciones y Nuevas Tecnologías de 23 de junio de 2022 sobre el proyecto de Orden citado en el encabezado, a los efectos de que se informara lo que proceda en relación con las competencias de esta Delegación y los aspectos relativos a la protección de datos que deban ser tenidos en cuenta en la política de seguridad de la información de esta Consejería, a continuación se pasan a analizar las observaciones puestas de manifiesto en el referido informe de 23 de junio de 2022, en relación con dichas cuestiones:

1) El informe indica que: *“Dado que se incluye en la composición del Comité, en el artículo 8 del proyecto de Orden, a la persona u órgano designado delegado o delegada de protección de datos de la Consejería, tener en consideración que, de conformidad con la Guía CCN-STIC 801 de Responsabilidades y Funciones, cuyo objeto es proponer un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los sistemas de información de las entidades del Sector Público del ámbito subjetivo de aplicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), desarrollando las figuras o roles más significativos que asuman dichas responsabilidades, “se deberá tener especial cuidado en analizar los posibles conflictos de intereses, muy especialmente en lo que se refiere al Delegado de Protección de Datos, que, en el ejercicio de sus funciones, no podrá recibir instrucciones, debiendo responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. La Política de Seguridad de la organización y los Términos de Referencia de este Comité deberán reflejar claramente las cautelas adoptadas en tal sentido, conforme a lo dispuesto en el precitado Informe Jurídico de la AEPD 2018-0170”.*

Al respecto, cabe señalar que, a la vista del artículo 38.1 del Reglamento General de Protección de Datos (*“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”*), así como a las funciones de asesoramiento, supervisión, etc. que el artículo 39 de la misma norma confiere al delegado de protección de datos en su ámbito compe-

Identificador: 20220715150415

Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre de los servicios electrónicos de confianza. Permite la verificación de la integridad de esta copia del documento electrónico en la dirección: [https://sede.gobiernodecanarias.org/sede/verifica\\_doc](https://sede.gobiernodecanarias.org/sede/verifica_doc)  
Este documento es una copia electrónica auténtica

Firmado por: Lourdes Maria Rodriguez Roldán

Fecha: 15/07/2022 15:06:10



XCfUvTdjvT4wuFonP1thlmoVuNZ3sg



Página: 1/4



tencial, se estima conveniente mantener la designación de la persona o unidad designada Delegada de Protección de Datos, como vocal del Comité previsto en el artículo 8 del proyecto de Orden.

Por otra parte, vistos el Reglamento General de Protección de Datos, especialmente su artículo 38, apartados 3 y 6, y la Ley Orgánica 3/2018, especialmente su artículo 36, apartado 2, así como la Guía CCN-STIC 801 y el informe AEPD 2018-0170, la posición de la persona o entidad delegada de protección de datos es diferente de la del responsable del tratamiento, ya que no determina la finalidad y medios del tratamiento, y de la del responsable de seguridad, ya que no puede decidir sobre los aspectos de seguridad en los sistemas de información. Al mismo tiempo, ha de preservarse la independencia del delegado de protección de datos en el ejercicio de sus funciones, sin que pueda recibir instrucciones ni estar incurso en conflicto de intereses, aplicándose las salvaguardas necesarias a tal fin.

Por lo que se entiende que procedería estimar esta alegación de la Dirección General de Telecomunicaciones y Nuevas Tecnologías, y se propone añadir un segundo párrafo al apartado 2.b) del artículo 8 del proyecto de Orden, con la siguiente redacción:

*“La persona o unidad designada Delegada de Protección de Datos de la Consejería participará en el Comité con voz, pero sin voto, en el marco de sus funciones de asesoramiento en materia de protección de datos, respetándose su independencia en el ejercicio de las competencias que le atribuye la normativa de protección de datos”.*

**2)** El informe indica que: *“En el artículo 17 o en el artículo 19 del proyecto de Orden relativos a la Gestión de riesgos, y a la Protección de datos de carácter personal, respectivamente, debería incluir, de conformidad con el apartado f) del artículo 12.1 del ENS, los riesgos que se deriven del tratamiento de los datos personales. Para ello, y en relación con el artículo 3 del ENS, se deberá prever la realización de los análisis de riesgos y, en su caso, evaluaciones de impacto, por parte de los responsables de los tratamientos de los datos de carácter personal”.*

Al respecto, cabe señalar que:

El artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, determina lo siguiente:

*“Artículo 3. Sistemas de información que traten datos personales.*

*1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protec-*

Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre de los servicios electrónicos de confianza. Permite la verificación de la integridad de esta copia del documento electrónico en la dirección: [https://sede.gobiernodecanarias.org/sede/verifica\\_doc](https://sede.gobiernodecanarias.org/sede/verifica_doc)  
Este documento es una copia electrónica auténtica

Firmado por: Lourdes Maria Rodriguez Roldán

Fecha: 15/07/2022 15:06:10



XCFuVTdjvT4wuFonP1thlmoVuNZA3sg



Página: 2/4



ción de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

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

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

Y, según el artículo 12.1 de la misma norma:

“Artículo 12. Política de seguridad y requisitos mínimos de seguridad.

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales”.

Ello en relación con la Disposición Adicional Primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, del siguiente tenor:

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

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

Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre de los servicios electrónicos de confianza. Permite la verificación de la integridad de esta copia del documento electrónico en la dirección: [https://sede.gobiernodecanarias.org/sede/verifica\\_doc](https://sede.gobiernodecanarias.org/sede/verifica_doc)  
Este documento es una copia electrónica auténtica

Firmado por: Lourdes Maria Rodriguez Roldán

Fecha: 15/07/2022 15:06:10



XCFuVTdjvT4wuFonP1thlmoVuNZA3sg



Página: 3/4



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

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

Al respecto, dado que el citado artículo 12.1 del Real Decreto 311/2022 incluye expresamente a los riesgos que se deriven del tratamiento de los datos personales como parte integrante de la Política de Seguridad, y que ha de gestionarse el riesgo tanto para los sistemas de información en general como para los datos personales en particular, aplicándose en cualquier caso las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, se entiende que procedería estimar esta alegación de la Dirección General de Telecomunicaciones y Nuevas Tecnologías.

Por lo que se propone modificar la redacción de los artículos 17 y 19 del proyecto de Orden, tal como se ha consensuado con el Servicio de Modernización y Nuevas Tecnologías, en los siguientes términos:

- Añadir, en el artículo 17, un apartado 5, del siguiente tenor:

*“5. Cuando un sistema de información trate datos personales, además de lo previsto en los apartados anteriores, el centro directivo responsable del tratamiento 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.*



*Todos los sistemas de información de la Consejería se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos personales. En caso de conflicto de esta con la normativa de seguridad, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de datos personales. Igualmente, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto previstos en este apartado, en caso de resultar agravadas respecto de las previstas en virtud de los apartados anteriores”.*

- Dar la siguiente redacción al artículo 19, que constará ahora de un único apartado:

*“En lo que se refiere a las operaciones de tratamiento de datos de carácter personal, estarán referenciados en el correspondiente registro de las actividades de tratamiento donde se harán constar tanto las actividades afectadas como las personas responsables correspondientes, así como la información requerida conforme a la normativa vigente en materia de protección datos”.*

Es cuanto se informa, sin perjuicio de todo otro criterio mejor fundado en Derecho.

## LA DELEGADA DE PROTECCIÓN DE DATOS

Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 6/2020, de 11 de noviembre de los servicios electrónicos de confianza Permite la verificación de la integridad de esta copia del documento electrónico en la dirección: <a href="https://sede.gobiernodecanarias.org/sede/verifica_doc">https://sede.gobiernodecanarias.org/sede/verifica_doc</a> Este documento es una copia electrónica auténtica	
Firmado por: Lourdes María Rodríguez Roldán	Fecha: 15/07/2022 15:06:10
 XCFuVTdjvT4wuFonP1thlmoVuNZA3sg	 Pagina: 4/4