



**Gobierno  
de Canarias**

Consejería de Administraciones  
Públicas, Justicia y Seguridad  
Dirección General de Telecomunicaciones  
y Nuevas Tecnologías

DGTNT-021910-TSI-RJO-INPR  
PSI CDSIDJ nuevo ENS

Página 1 de 8

Régimen Jurídico y Asuntos Generales/ Telecomunicaciones y  
Sistemas de Información

Estado: Definitivo

**INFORME SOBRE EL PROYECTO DE ORDEN DE LA CONSEJERÍA DE  
DE DERECHOS SOCIALES, IGUALDAD, DIVERSIDAD Y JUVENTUD,  
POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA  
INFORMACIÓN EN EL ÁMBITO DE LA ADMINISTRACIÓN  
ELECTRÓNICA DE ESA CONSEJERÍA.**

| Rev.   | Fecha      | Descripción   |                              |
|--|------------|---|------------------------------|
| 01   | 01/06/2022 | Informe sobre el Proyecto de Orden de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración electrónica de esa Consejería |                              |
|  |            |   |                              |
|  |            |   |                              |
|  |            |   |                              |
| <b>Documento:</b>  |            | DGTNT-021910-TSI-RJO-INPR- PSI CDSIDJ nuevo ENS   |                              |
| <b>Ubicación en eCarpeta:</b>  |            | <a href="https://www.gobiernodecanarias.net/eCarpeta/faces/jsp/browse/browse.jsp">https://www.gobiernodecanarias.net/eCarpeta/faces/jsp/browse/browse.jsp</a>   |                              |
| <b>Nivel de Seguridad:</b>   |            | Restringido   |                              |
| <b>Preparado por</b>   |            | <b>Revisado por</b>   | <b>Aprobado por</b>          |
| M. <sup>a</sup> Elena Prieto Gámez<br>M. <sup>a</sup> Elena Ruano Rivero |            | José Damián Ferrer Quintana   | Víctor Manuel Melián Santana |



## ÍNDICE

|                              |          |
|------------------------------|----------|
| <b>1. INTRODUCCIÓN.....</b>  | <b>3</b> |
| <b>2. ÁMBITO.....</b>        | <b>3</b> |
| <b>3. DESTINATARIOS.....</b> | <b>3</b> |
| <b>4. INFORME.....</b>       | <b>3</b> |
| <b>5. CONCLUSIONES.....</b>  | <b>8</b> |
| <b>6. CONTACTOS.....</b>     | <b>8</b> |



## 1. INTRODUCCIÓN

Recibida petición de informe por parte de la Secretaría General Técnica de Derechos Sociales, Igualdad, Diversidad y Juventud, con fecha 25 de mayo de 2022, en relación al Proyecto de Orden de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la Administración electrónica de esa Consejería, se emite el siguiente informe en cumplimiento de lo dispuesto en el artículo 2.3 de la Orden de la Consejería de Presidencia, Justicia e Igualdad, de 31 de julio de 2013, por la que se establece el marco común y las directrices básicas de la política de seguridad de la información en el ámbito de la Administración Electrónica de la Administración Pública de la Comunidad Autónoma de Canarias.

## 2. ÁMBITO

Dada la entrada en vigor del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y que deroga 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, es de aplicación la nueva normativa.

## 3. DESTINATARIOS

El informe será remitido a la Secretaría General Técnica de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud.

## 4. INFORME

El artículo 12, en sus apartados 1 y 2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante ENS, establece:

*“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.*

*2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.*

*No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.”*

El apartado 2 del artículo 13 del ENS recoge:

*“2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:*

a) *El responsable de la información determinará los requisitos de la información tratada*

b) *El responsable del servicio determinará los requisitos de los servicios prestados.*

c) *El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.*

d) *El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.”*

- El proyecto de Orden, remitido recoge en su artículo 1:

**“Artículo 1.- Objeto y ámbito de aplicación.**

1. La presente Resolución tiene por objeto establecer la Política de Seguridad de la Información (en adelante, PSI), en el ámbito de la administración electrónica de la Consejería de Derechos Sociales, Igualdad, Diversidad y Juventud (en adelante, la Consejería).

2. La PSI aprobada se aplicará a todos los servicios, aplicaciones o sistemas de la Consejería, por todo el personal de las unidades administrativas de este departamento, así como por el personal de otros organismos o entidades que hayan sido autorizados para acceder a los sistemas de información incluidos en su ámbito de aplicación.



3. La PSI de esta Consejería debe ser observada por las personas físicas, jurídicas y entes sin personalidad en sus relaciones con las entidades anteriores cuando procedan al uso de sus sistemas de información.”

- Así mismo, el proyecto de Orden, remitido recoge en su artículo 7:

**“Artículo 7.- Organización de la seguridad.**

1. La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la administración electrónica de la Consejería está compuesta por los siguientes agentes:

- a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.
- b) Una o varias personas Responsables de la Información.
- c) Una o varias personas Responsables de los Servicios Públicos prestados a la Ciudadanía.
- d) Una persona Responsable de Seguridad de la Información.
- e) Una o varias personas Responsables del Sistema de la Información.

2. La designación de las personas señaladas en las letras b), c), d) y e) corresponderá a la persona titular de la Secretaría General Técnica del Departamento, y de la Dirección de cada organismo público dependiente de la Consejería a los que les sea de aplicación esta PSI, de acuerdo con su propia organización interna.”

El ámbito de aplicación deberá quedar claramente definido en la propia Política de Seguridad de la Información en su artículo 1.

Conforme al artículo 12.2 del ENS cada órgano o entidad con personalidad jurídica propia deberá contar con una política de seguridad formalmente aprobada por el órgano competente. No obstante, los organismos públicos podrán quedar incluidos en el ámbito subjetivo de la política de seguridad del Departamento, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización. Así mismo, el apartado 2 del artículo 7 del proyecto de Orden, debe ser coherente y claro respecto a su ámbito de aplicación establecido en el artículo 1.

Por lo expuesto, deberá quedar claramente establecido el ámbito de aplicación de la PSI en su artículo 1, respecto a los organismos incluidos o no; y, adecuar a ese ámbito de aplicación la redacción del resto del articulado.

La Política de Seguridad de la Información debe ser un documento que establezca claramente las distintas funciones o roles en materia de seguridad en su ámbito de aplicación, así como los respectivos deberes y responsabilidades, por lo que es indeterminado una propuesta de “Una o varias” personas.

Así mismo, si la designación de los distintos roles recae en la Secretaría General Técnica de ese Departamento, es incongruente con el resto del articulado del proyecto de Orden, el cual concreta el Responsable de Seguridad y Responsable del Sistema en la propia Política de Seguridad de la Información.

No obstante, debería hacerse referencia conforme al letra c) del artículo 11.1 del ENS, al procedimiento para su designación y renovación, de conformidad con el régimen jurídico correspondiente en las administraciones públicas.



- 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”*.

- El apartado 2 del artículo 10 del proyecto de Orden, relativo a los **Responsables de la Información**, propone:

“2. Esta responsabilidad recaerá en la persona titular del órgano que gestione cada procedimiento, trámite o cualquier otro servicio electrónico.”

Las personas Responsables de la Información no son responsables de determinar los requisitos de seguridad de los servicios electrónicos prestados, sino de determinar los requisitos de seguridad de la información tratada. Este extremo corresponderá a las personas Responsables de los Servicios, por lo que deberá aclararse dicho apartado.

- El artículo 12 del Proyecto de Orden, relativo al **Responsable de Seguridad**, propone en su apartado 3, m):

“m) Proponer la Declaración de Conformidad, para su aprobación por la persona titular del Departamento, previo informe del Comité para la Gestión y Coordinación de la Seguridad de la Información”

Debe tenerse en consideración que la Declaración de Conformidad o, en su caso, Certificación de Conformidad, dependerá de la categorización del sistema de información.

- Respecto al apartado 4 del artículo 12 del proyecto de Orden, relativo al **Responsable de Seguridad** recoge:

“4. Cuando la complejidad, distribución, separación física de sus elementos o número de personas usuarias de los sistemas de información lo justifiquen, la persona Responsable de Seguridad podrá designar tantas personas responsables de seguridad delegadas como se necesiten, que tendrán dependencia funcional directa, y que adquirirán responsabilidad en su ámbito de todas



aquellas acciones que les sean delegadas. Para el ejercicio de sus funciones podrá contar con el asesoramiento y apoyo del Comité para la Gestión y Coordinación de la Seguridad de la Información.”

Debe aclararse que, de conformidad con la Guía CCN -CERT 801 de Responsabilidades y Funciones, determinadas funciones podrán delegarse, pero la responsabilidad es indelegable, por lo que deberá corregirse tal indicación. Así mismo, en el mismo sentido, deberá adecuarse lo recogido en el artículo 13.4 del proyecto de Orden relativo al **Responsable del Sistema de la Información**.

- El artículo 13 del proyecto de orden, dedicado al Responsable del Sistema de Información recoge en su apartado 2:

“2. Los sistemas de información propios de esta Consejería se alojarán en la infraestructura tecnológica corporativa preferiblemente en servidores cibergestionados y, en caso de ser necesario, autogestionados.”

Es necesario eliminar el término cibergestionados, dado que este tipo de servidores o servicios no existen según la Normativa de Gestión de Alojamiento de Aplicaciones.

- Respecto al artículo 16 del proyecto de Orden, dedica a **Terceras partes**, se deberá tener en consideración en la redacción de dicho artículo que, conforme al artículo 2.3 del ENS, dicha norma “ ... también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

*La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.*

*Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.*

*Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.”*

- 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.

- El artículo 18 del proyecto de Orden recoge los aspectos relativos al “Desarrollo normativo de la PSI. Documentación de la seguridad”. Conforme a la letra e) del artículo 12.1 del ENS, establece unas directrices para la estructuración de la documentación en tres niveles. No obstante, respecto a “su gestión y acceso”, si bien asigna esta responsabilidad al Responsable de Seguridad, no se aclara donde estará ubicada esta documentación, ni los mecanismos de acceso a la misma.

## 5. CONCLUSIONES

Por todo lo expuesto, debería adecuarse el proyecto de Orden remitido a las indicaciones expuestas en el presente informe, y al Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad.

## 6. CONTACTOS

Persona de contacto José Damián Ferrer Quintana  
Puesto Jefe de Área de Telecomunicaciones y Sistemas  
Teléfono 58358  
Correo electrónico [jferqui@gobiernodecanarias.org](mailto:jferqui@gobiernodecanarias.org)

Persona de contacto María Elena Ruano Rivero  
Puesto Jefe de Sección de Seguridad  
Teléfono 58472  
Correo electrónico [mruarivr@gobiernodecanarias.org](mailto:mruarivr@gobiernodecanarias.org)

Persona de contacto María Elena Prieto Gámez  
Puesto Jefe de Sección de Procedimiento de Seguridad  
Teléfono 58476  
Correo electrónico [mprigam@gobiernodecanarias.org](mailto:mprigam@gobiernodecanarias.org)

Este documento ha sido firmado electrónicamente por:

VICTOR MANUEL MELIAN SANTANA - DIRECTOR/A GENERAL  
JOSE DAMIAN FERRER QUINTANA - JEFE AREA TELECOMUNICAC.Y SISTEMAS  
MARIA ELENA RUANO RIVERO - J/SECCION DE SEGURIDAD  
MARIA ELENA PRIETO GAMEZ - J/SEC.PROCEDIMIENTO DE SEGURIDAD

Fecha: 23/06/2022 - 11:32:06  
Fecha: 23/06/2022 - 08:40:28  
Fecha: 23/06/2022 - 08:03:03  
Fecha: 22/06/2022 - 15:02:04

En la dirección [https://sede.gobiernodecanarias.org/sede/verifica\\_doc?codigo\\_nde=](https://sede.gobiernodecanarias.org/sede/verifica_doc?codigo_nde=)  
puede ser comprobada la autenticidad de esta copia, mediante el número de  
documento electrónico siguiente:

0VVbc13snt46K32dIKx9trgvWnCNfNUGU



El presente documento ha sido descargado el 30/06/2022 - 10:36:59