Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

INFORME DE LA COMISIÓN CONSULTIVA DE LA TRANSPARENCIA Y LA PROTECCIÓN DE DATOS DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA, AL PROYECTO DE ORDEN DE LA CONSEJERÍA DE UNIVERSIDAD, INVESTIGACIÓN E INNOVACIÓN POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD INTERIOR Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN EL ÁMBITO DE LA CONSEJERÍA Y DE SUS ENTIDADES ADSCRITAS.

I.- Con fecha 10 de octubre de 2023 ha tenido entrada en el Consejo de Transparencia y Protección de Datos de Andalucía solicitud de informe, efectuada por la Consejería de Universidad, Investigación e Innovación, referente al proyecto de Orden por la que se establece la política de seguridad interior y seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.

Con la petición de informe se acompaña el proyecto de Orden así como la Memoria justificativa y económica, la Memoria justificativa del cumplimiento de los principios de buena regulación y el Acuerdo de inicio de la tramitación del expediente sobre el proyecto de Orden.

II.- La Comisión Consultiva de la Transparencia y la Protección de Datos emite el presente informe preceptivo de acuerdo con lo previsto en el artículo 15.1.d) de los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre, y con el artículo 57 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en relación con el artículo 57.1.c) del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Este informe se refiere exclusivamente a aquellas cuestiones que, tras el análisis del texto de la norma proyectada, afectan, a juicio de esta Comisión, a materias relacionadas directamente, o por conexión, con la transparencia pública y la protección de datos personales. No se realizan, por tanto, consideraciones sobre otros aspectos generales o mejoras de técnica normativa, que deberán ser informados, en su caso, por los órganos que sean competentes.

III.- La normativa tomada en consideración para la elaboración del presente informe, a la que ha de ajustarse el proyecto sometido a consulta, está integrada, en materia de transparencia, por la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (en adelante LTPA), la Ley 19/2013, de

9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (en adelante LTAIBG) y los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, ya citados.

Y, en materia de protección de datos personales, además de las normas mencionadas en el párrafo anterior, son de aplicación el citado Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), así como la Ley Orgánica 3/2018, de 5 de diciembre (en adelante LOPDGDD), ya citada.

Todo ello sin perjuicio de tomar en consideración cualquier otra norma que pueda ser aplicable por su relación con cuestiones concretas de este informe.

IV.- Sobre el texto remitido pueden realizarse las siguientes consideraciones:

1. Con carácter general, numeración errónea del articulado.

En la numeración de los artículos del proyecto de Orden se observa un error: tras el artículo 9 aparece el art. 11, después del mismo figura el art. 10 y, a continuación, un segundo art. 11, siguiendo a continuación el art. 13.

Por razones de claridad, en el presente informe se mantiene la numeración del texto remitido para informe.

2. Con carácter general, uso de la expresión "datos personales".

Se sugiere que a lo largo de todo el texto del proyecto de Orden se sustituya la expresión "datos de carácter personal" por la de "datos personales", por ser más acorde con la terminología empleada en la normativa vigente, en especial, por el artículo 4.1) del RGPD así como por el propio título de la LOPDGDD.

3. Sobre el "artículo 1. Objeto."

El art. 1 del proyecto de Orden dispone lo siguiente:

"*1. La presente orden tiene por objeto definir y regular la política de seguridad interior de la Consejería de Universidad, Investigación e Innovación que defina el sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios.*

2. También es objeto de la misma definir y regular la política de seguridad de las tecnologías de la información y las comunicaciones (en adelante, seguridad TIC) de la Consejería, y constituye su documento de política de seguridad TIC."

Este precepto no incluye dentro de su objeto, de forma explícita, la protección de datos personales, a pesar de que el proyecto de Orden dedica su capítulo III (arts. 37 a 44) a dicha materia. Se sugiere incorporar esta dimensión dentro del objeto.

4. Sobre el "artículo 3. Marco regulador."

El art. 3 del proyecto de Orden establece:

"*1. Se asume como marco regulador en materia de seguridad interior el establecido en el artículo 15 del Decreto 171/2020, de 13 de octubre, por el que se establece la política de seguridad interior en la Administración de la Junta de Andalucía, de conformidad con lo que establezca el Comité Corporativo de Seguridad, y en materia de seguridad TIC el que en cada momento se defina, en virtud de la disposición adicional primera del Decreto 1/2011, de 11 enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, por la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones, a propuesta del Comité de Seguridad TIC de la Junta de Andalucía. Todo ello, sin perjuicio de otra normativa aplicable a la Consejería de Universidad, Investigación e Innovación en virtud de su naturaleza legal y de sus competencias.*

2. La Consejería de Universidad, Investigación e Innovación podrá ampliar y desarrollar el marco regulador de la seguridad TIC, teniendo en cuenta lo previsto en la disposición adicional 1.ª 1.a) del Decreto 1/2011, de 11 de enero."

Se sugiere incluir, de forma explícita, dentro del marco regulador, el vigente en materia de protección de datos. En concreto, podría incluirse al **final del apartado 1**, con la siguiente redacción, u otra similar:

"así como la normativa vigente en materia de protección de datos: 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), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y demás disposiciones que resulten de aplicación."

5. Sobre el "artículo 5. Contexto."

El art. 5 del proyecto de Orden señala:

"*La seguridad interior implica a todas las áreas de la Consejería, al desplegarse para la prevención de daños intencionales sobre su personal y personas usuarias, sobre sus activos y sobre la continuidad de su funcionamiento y servicios, así como para la reacción cuando tales daños se produzcan.*

La seguridad de la información implica prácticamente a todas las áreas de la Consejería Universidad, Investigación e Innovación, habida cuenta de que ha de estar presente en todos los ámbitos de su actividad y debe tener un carácter multidisciplinar, abarcando áreas como la informática y comunicaciones, gestión de personal y financiera o ejecución de proyectos."

Se sugiere incluir en la **frase final del segundo párrafo**, como otra área comprendida, la protección de datos personales.

6. Sobre el "artículo 6. Obligaciones generales."

El art. 6 del proyecto de Orden dice:

"*1. Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para afectar a la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.*

2. Las unidades organizativas, entendiéndose por tal órganos y unidades administrativas, deben cumplir los requisitos mínimos de seguridad exigidos en el Esquema Nacional de Seguridad (en adelante, ENS). En concreto, los requisitos mínimos son los siguientes:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal. Se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los sistemas de información de la Consejería conozca sus responsabilidades, y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Profesionalidad. La seguridad de los sistemas de información estará atendida, revisada y auditada por personal cualificado.

e) Autorización y control de los accesos. Se limitará el acceso a los activos de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes con su calificación.

f) Protección de las instalaciones. Los sistemas de información estarán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su criticidad. Los locales donde se ubiquen los sistemas dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado.

g) Adquisición de productos y contratación de servicios de seguridad. Las diferentes unidades organizativas identificarán los requisitos de seguridad a incluir para la adquisición de productos o contratación de servicios de seguridad.

h) Mínimo privilegio. Otorgar a los usuarios los permisos estrictamente necesarios sobre los sistemas y la información para el desempeño de sus funciones en el organismo según sus perfiles individuales y específicos, eliminando cualquier función innecesaria o inadecuada para conseguir este fin. Las funciones de operación y administración serán desarrolladas exclusivamente por el personal autorizado.

i) Integridad y actualización del sistema. Se requerirá una autorización formal previa a la instalación de un sistema por parte del responsable del servicio. Se deberá conocer el estado de la seguridad del sistema en relación con las recomendaciones y actualizaciones de seguridad recomendadas por el fabricante.

j) Protección de la información almacenada y en tránsito. Toda la información almacenada de forma centralizada será periódicamente respaldada. La información que se transmita a través de redes de comunicaciones o soportes portátiles estará adecuadamente protegida, teniendo en cuenta su calificación y criticidad, mediante mecanismos que garanticen su seguridad.

k) Prevención ante otros sistemas de información interconectados. Se dispondrá de un sistema de cortafuegos que separe la red interna del exterior. Todo el tráfico atravesará dicho cortafuegos y solo se dejará transitar los flujos previamente autorizados. Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información alguna.

l) Registro de actividad y detección de código dañino. Se registrarán aquellos eventos que se consideren de interés, tanto para la detección de actividades que puedan comprometer la seguridad, como para dejar constancia de aquellas otras actividades que permitan verificar y evidenciar la efectividad de los controles, las normas de seguridad establecidas por la Consejería y los requisitos legales aplicables.

m) Incidentes de seguridad.

n) Continuidad de la actividad. Las unidades organizativas deberán elaborar planes de continuidad del negocio. Se implantarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información teniendo en cuenta la valoración de la dimensión de disponibilidad.

ñ) Mejora continua del proceso de seguridad. Se elaborarán planes de mejora continua que se presentarán para su aprobación al Comité de Seguridad TIC.

3. Las unidades organizativas deberán realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades organizativas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Así, los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC. Las unidades organizativas deben estar preparadas para prevenir, detectar, responder y recuperarse de los incidentes de seguridad.

4. Las reglas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por la Consejería de Universidad, Investigación e Innovación y a los demás instrumentos jurídicos en los que se vertebre cualquier prestación de servicios TIC a la misma.

5. Toda la documentación generada para el desarrollo de proyectos TIC tendrá la obligación de utilización de un lenguaje no sexista."

En conexión con el artículo 3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se proponen las siguientes modificaciones:

a) Introducir **entre los apartados 1 y 2** actuales un nuevo apartado, que haga mención a que cuando los sistemas de información traten datos personales debe aplicarse lo dispuesto en la normativa vigente en materia de protección de datos, así como las recomendaciones y directrices dictadas por el Consejo de Transparencia y Protección de Datos de Andalucía, en materia de protección de datos.

b) Redactar el **apartado 2, letra b)**, de la siguiente forma: "Análisis y gestión de los riesgos. En los supuestos de sistemas de información que traten datos personales se realizará, con el asesoramiento

del delegado de protección de datos, 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 relativa a la protección de datos."

7. Sobre el "artículo 8. Detección."

El art. 8 del proyecto de Orden indica:

"1. Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple ralentización hasta su detención, se deberán monitorizar de manera continua para detectar anomalías en los niveles de prestación de los mismos y actuar en consecuencia según lo establecido en el ENS.

2. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo dispuesto en el ENS. Así, se establecerán mecanismos de detección, análisis y reporte que lleguen a las personas responsables tanto de una manera regular, como cuando se produzca alguna desviación significativa de los parámetros que se hayan preestablecido como normales."

Para valorar si un incidente o anomalía afecta a datos personales, se sugiere añadir al **final del apartado 1**, la siguiente frase: "Si la anomalía detectada afectase a datos personales, se contactará con el responsable del tratamiento que actuará de acuerdo con lo establecido en el artículo 40 de la presente Orden, relativo a la violación de la seguridad de los datos personales."

8. Sobre el "artículo 9. Respuesta."

El art. 9 del proyecto de Orden dispone:

"*Las unidades organizativas deben:*

a) Colaborar con el equipo de gestión de incidentes de seguridad de la Consejería de Universidad, Investigación e Innovación.

b) Designar un punto de contacto para las comunicaciones relativas a incidentes detectados en otras unidades organizativas o en otros organismos.

c) Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta ante Emergencias Informáticas."

Se sugiere incluir al **final de la letra a)**, la siguiente expresión: "[...] y con el delegado de protección de datos, en caso de que se vean afectados datos personales".

9. Sobre el "artículo 11. Estructura organizativa de la seguridad interior y seguridad TIC." (segundo artículo del proyecto de Orden con esta numeración).

El art. 11 del proyecto de Orden, relativo a la estructura organizativa de la seguridad interior y seguridad TIC, establece:

"*1. La gestión de la seguridad interior y seguridad de la información va íntimamente ligada al establecimiento de una organización de seguridad. Dicha organización se establece mediante la identificación de las diferentes actividades y responsabilidades en materia de gestión de la seguridad y mediante su asignación formal a los agentes que correspondan, con arreglo al principio de básico de función diferenciada recogido tanto en el ENS como en la política de seguridad interior y seguridad TIC de la Junta de Andalucía.*

2. Atendiendo a dicho principio, la estructura que se define en este documento diferencia cuatro bloques de responsabilidad:

a) La especificación de las necesidades y requisitos en materia de seguridad de la información.

b) El desarrollo y/o explotación del sistema de información.

c) La función de supervisión de la seguridad del sistema de información.

d) La determinación de activos-tipo en el ámbito de la Consejería, el análisis de riesgos, los niveles de protección objetivo y los tipos de medidas de seguridad pertinentes para los riesgos-tipo en los activos de su ámbito.

En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente sobre los distintos agentes integrantes de la siguiente estructura organizativa en dos niveles:

a) En la Consejería de Universidad, Investigación e Innovación:

1.º Comité de Seguridad Interior y Seguridad TIC.

2.º Las personas responsables de la información.

3.º Las personas responsables del servicio.

4.º La Unidad de Seguridad TIC.

5.º La Unidad de Seguridad Interior.

6.º La persona responsable de seguridad TIC.

7.º Las personas responsables del sistema.

Además, de conformidad con lo establecido en la normativa sobre protección de datos personales, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas con la seguridad TIC:

8.º La figura del responsable del tratamiento.

9.º La figura del encargado del tratamiento.

b) En cada una de las entidades vinculadas o dependientes:

1.º Comité de Seguridad Interior y Seguridad TIC.

2.º Las personas responsables de la información.

3.º Las personas responsables del servicio.

4.º La persona responsable de seguridad TIC.

5.º Las personas responsables del sistema.

6.º La Unidad de seguridad Interior en caso de que se constituya en aquellas entidades dependientes en las que éstas lo consideren necesario por virtud del volumen o singularidad de los activos.

En ambos niveles, el delegado de protección de datos informará y asesorará a los responsables y encargados del tratamiento y supervisará el cumplimiento de lo dispuesto en la normativa de protección de datos.

3. Dependiendo de las necesidades y circunstancias de la organización, en ciertos casos, la función de algunos de estos agentes podrá recaer sobre una misma persona, unidad o departamento.

4. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la política de seguridad TIC de la Junta de Andalucía y por su normativa de desarrollo, en las entidades vinculadas o dependientes de la Consejería de Universidad, Investigación e Innovación, la responsabilidad de la conformación y designación de estas figuras recaerá sobre las propias entidades vinculadas o dependientes.

En el **inciso final del apartado 1**, cuando se dice: "...c*on arreglo al principio de básico*...", sobra la proposición "de".

El **apartado 2** no incluye dentro de los bloques de responsabilidad la protección de datos. En conexión con el comentario efectuado al artículo 1 (apartado IV. 3 de este informe), se aconseja incluir la protección de datos como un bloque específico comprendido dentro de los bloques de responsabilidad.

10. Sobre el "artículo 13. Creación y composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación."

El art. 13 del proyecto de Orden señala:

"*1. Se crea el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación para la dirección y seguimiento en materia de seguridad interior en todos sus ámbitos de actuación y en materia de seguridad de los activos TIC de los que dicha Consejería sea titular o cuya gestión tenga encomendada.*

2. El Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación estará compuesto por los siguientes miembros:

a) La presidencia le corresponderá a la persona titular de la Viceconsejería, la cual tendrá voto de calidad en la toma de decisiones del Comité en caso de empate.

b) La vicepresidencia, que será ejercida por la persona titular de la Secretaría General Técnica.

c) Las vocalías, que serán desempeñadas por:

1.º La persona titular de cada uno de los órganos directivos centrales de la Consejería de Universidad, Investigación e Innovación.

2.º La persona titular de la Coordinación General de la Secretaría General Técnica.

d) La secretaría será ejercida por la persona titular de la Jefatura de Sistemas de Información Sectoriales de Innovación y Sostenibilidad, con voz y voto.

3. El delegado de protección de datos y las personas responsables de las Unidades de Seguridad Interior y Seguridad TIC podrán asistir en calidad de personas asesoras a las reuniones del Comité de Seguridad Interior y Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia.

4. La composición del Comité de Seguridad Interior y Seguridad TIC, teniendo en cuenta a sus suplentes, deberá tener una representación equilibrada entre hombres y mujeres, conforme a lo establecido en los artículos 3.3 y 11.2 de la Ley 12/2007, de 26 de noviembre. No podrán participar en el mismo aquellas personas que hayan sido condenadas por razón de violencia de género o sobre las que haya recaído sanción por resolución firme en vía administrativa o sentencia judicial firme por razón de discriminación en prácticas laborales.

5. En caso de vacante, ausencia, enfermedad y, en general, cuando concurra una causa justificada, la persona titular de la presidencia podrá ser sustituida por la persona titular de la vicepresidencia. La vicepresidencia y las vocalías podrán ser sustituidas por la persona suplente que la titular designe mediante acto documentado que remitirá al Comité de Seguridad Interior y Seguridad TIC. La persona titular de la secretaría podrá ser sustituida por la persona funcionaria que designe la presidencia del Comité de Seguridad Interior y Seguridad TIC."

Dada la especial relevancia que los asuntos tratados en el Comité de Seguridad Interior y Seguridad TIC de la Consejería tiene para la protección de datos, se sugiere incluir en el **apartado 2** la participación del delegado de protección de datos como miembro del citado Comité, sin condicionar la misma a las decisiones de la presidencia del Comité.

Además, para garantizar que sus funciones y cometidos no den lugar a conflicto de intereses, se propone que la asistencia del delegado de protección de datos al citado Comité lo sea en calidad de asesor, con voz pero sin voto, no quedando de esta forma involucrado en la toma de decisiones del Comité.

11. Sobre el "artículo 14. Funciones del Comité de Seguridad Interior y Seguridad TIC."

El art. 14 del proyecto de Orden indica:

"*1.En relación con las funciones de seguridad interior, el Comité de Seguridad Interior y Seguridad TIC tendrá asignadas las siguientes funciones:*

a) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos para la seguridad interior, incluido el Plan de Seguridad Interior de la Consejería.

b) Impulsar el cumplimiento de la política de seguridad interior.

c) Velar por la disponibilidad de los recursos para el desarrollo de los objetivos e iniciativas definidas en el Plan de Seguridad Interior de la Consejería.

d) Atender las peticiones en materia de seguridad interior de los centros directivos.

e) Establecer el modelo de relación con los Puntos Coordinadores de Seguridad Interior.

f) Determinar las condiciones y requisitos mínimos que deben contener los Planes de Seguridad Interior de las entidades adscritas a la Consejería, a propuesta de la Unidad de Seguridad interior de la Consejería.

g) Establecer directrices comunes y supervisar el cumplimiento de la normativa de seguridad interior en el ámbito de la Consejería.

h) La designación de la persona responsable de la Unidad de Seguridad Interior de la Consejería.

i) Promover programas de formación, entrenamiento y concienciación sobre las medidas relativas a la seguridad interior entre el personal de la Consejería.

j) Cualquier otra que se le asigne, por órgano o normativa competente, en materia de seguridad interior.

2. En relación con la seguridad TIC, el Comité de Seguridad Interior y Seguridad TIC tendrá asignadas las siguientes funciones:

a) Impulsar el cumplimiento de la política de seguridad TIC y su desarrollo normativo, estableciendo las directrices *comunes y de supervisión de seguridad TIC.*

b) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC, velando, en particular, por la coordinación entre diferentes planes que puedan coexistir. Además, le corresponde promover la mejora continua del sistema de gestión de la seguridad TIC.

c) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

d) Nombrar a las personas que formarán la Unidad de Seguridad TIC, garantizando el principio de función diferenciada.

e) Nombrar a la persona responsable de seguridad TIC.

f) Nombrar a las personas responsables del sistema.

g) Impulsar el cumplimiento de la política de seguridad TIC.

h) Atender las peticiones en materia de seguridad TIC de los centros directivos.

i) Informar regularmente a la persona titular de la Consejería de Universidad, Investigación e Innovación del estado de la seguridad de las TIC en su ámbito.

j) Elevar las propuestas de revisión de la política de seguridad TIC de la Consejería de Universidad, Investigación e Innovación, de sus directrices y sus normas de seguridad, así como del marco normativo de seguridad TIC de la Administración de la Junta de Andalucía, a los órganos competentes para su tramitación.

k) Aprobar las normas generales de seguridad TIC, además de la normativa de segundo y tercer nivel de seguridad TIC de la Consejería de Universidad, Investigación e Innovación.

l) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad TIC para asegurar que son consistentes y están alineados con la estrategia decidida, evitando duplicidades.

m) Realizar tareas de coordinación de los comités de Seguridad Interior y de Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería de Universidad, Investigación e Innovación.

n) Promover la formación, el entrenamiento y la concienciación de las medidas legales y organizativas relativas a la seguridad TIC entre el personal de Consejería de Universidad, Investigación e Innovación.

ñ) Elaborar y aprobar los requisitos de formación y cualificación de las personas administradoras, operadoras y usuarias desde el punto de vista de seguridad TIC de la Consejería de Universidad, Investigación e Innovación.

o) Coordinar y aprobar los planes de continuidad de la Consejería de Universidad, Investigación e Innovación.

p) Promover auditorías periódicas para verificar el correcto cumplimento de la política, la normativa y los procedimientos de seguridad.

q) Monitorizar los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de los mismos.

r) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos, velando, en particular, por la coordinación en la gestión de incidentes de la seguridad TIC.

s) Priorizar las actuaciones en materia de seguridad TIC cuando los recursos sean limitados.

t) Velar para que la seguridad TIC se tenga en cuenta en todos los proyectos, desde su especificación inicial hasta su puesta en producción, procurando la creación y utilización de servicios horizontales que reduzcan duplicidades y permitan un funcionamiento homogéneo de todos los sistemas.

u) Resolver los conflictos de competencia que se puedan suscitar entre las diferentes personas responsables de la gestión de la seguridad TIC o elevar propuesta para resolverlos, en su caso.

v) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectarán a la seguridad de la información, todo ello con la participación de las personas responsables de la información, de la Unidad Seguridad TIC y con el asesoramiento de la persona delegada de protección de datos.

w) Impulsar los preceptivos análisis de riesgos, junto a las personas responsables de la información que correspondan, contando con la participación de la Unidad de Seguridad TIC y del asesoramiento de la persona delegada de protección de datos.

x) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y servicios de su competencia, obtenidos en los análisis de riesgos realizados.

y) Coordinar las medidas técnicas y organizativas establecidas en la normativa de protección de datos personales, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos, contando con el asesoramiento de la persona delegada de protección de datos."

En el **apartado 2, letra r)**, se sugiere añadir el siguiente inciso final: "… y por los riesgos que pudiera suponer para los datos personales". Ello supone incluir al Comité en la supervisión de la afección que un incidente de seguridad pudiera tener sobre los datos personales.

En el **apartado 2 letra y)**, se sugiere la siguiente redacción, por mostrarse más en consonancia con lo dispuesto en el RGPD: *"*Coordinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, las evaluaciones de impacto relativa a la protección de datos personales, contando con el asesoramiento del delegado de protección de datos*"*.

12. Sobre el "artículo 15. Funcionamiento del Comité de Seguridad Interior y Seguridad TIC."

El art. 15 del proyecto de Orden dice:

"*1.1. El Comité de Seguridad Interior y Seguridad TIC se reunirá con carácter ordinario, al menos, unas vez al año y, con carácter extraordinario, cuando lo decida la persona titular de la presidencia de oficio o a propuesta de alguno de sus personas miembros, y siempre que se produzca alguno de los siguientes supuestos:*

a) Se produzcan incidencias de seguridad graves que afecten a cualquier sistema o a la seguridad interior.

b) Surjan nuevas necesidades de seguridad que requieran la participación del Comité.

2. El Comité de Seguridad Interior y Seguridad TIC podrá constituirse, convocar y celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario.

3. Los miembros del Comité de Seguridad Interior y Seguridad TIC podrán proponer a la presidencia, individual o colectivamente, la inclusión de asuntos en el orden del día. La propuesta deberá realizarse a través de medios electrónicos, dirigido a la presidencia con una antelación mínima de dos días a la fecha de la convocatoria.

4. A las sesiones del Comité de Seguridad Interior y Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la presidencia, por iniciativa propia o a propuesta de sus personas miembros, sin que, en ningún caso, pueda ocasionar coste económico.

5. La persona que ostente la secretaría del Comité levantará acta de cada reunión del mismo."

El **apartado 1.1** debe ser numerado como apartado 1. Además, al **final de la primera línea** de este apartado la palabra "*unas*" debe figurar en singular.

Al objeto de reforzar las garantías de la información transmitida durante las sesiones a distancia del Comité de Seguridad Interior y Seguridad TIC, se propone modificar la redacción del **apartado 2** de forma que quede redactado de la siguiente forma:

"2. El Comité de Seguridad Interior y Seguridad TIC podrá constituirse, convocar y celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes, así como la integridad, confidencialidad y la autenticidad de la información entre ellas transmitidas, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario".

Asimismo, con idéntico motivo, se propone añadir en el **apartado 2**, a continuación del párrafo anterior, un párrafo con el siguiente tenor: "Los miembros del Comité de Seguridad Interior y Seguridad TIC están obligados a respetar la confidencialidad de toda la información a la que tengan acceso".

Además, considerando que la obligación de confidencialidad debe abarcar, asimismo, al personal asesor que pueda ser convocado a las reuniones del citado Comité, se aconseja completar la redacción del **apartado 4,** que quedaría como sigue:

"4. A las sesiones del Comité de Seguridad Interior y Seguridad TIC podrán asistir en calidad de asesoras, con voz pero sin voto, las personas que en cada caso estime pertinente la presidencia, por iniciativa propia o a propuesta de sus personas miembros, estando obligadas a respetar la confidencialidad de toda la información a la que tengan acceso, sin que, en ningún caso, pueda ocasionar coste económico."

13. Sobre el "artículo 17. Responsable de la información."

El art. 17 del proyecto de Orden dispone:

"*1. La figura de responsable de la información en lo relativo al ENS, es aquella quien tiene la información y determinará sus niveles de seguridad dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y Salud, siendo posible la presentación de una propuesta previa por parte del Comité de Seguridad Interior y Seguridad TIC.*

2. La persona en quien recaerá la figura de responsable de la información, y de acuerdo con la guía de seguridad CCN-STIC-801 que trata las responsabilidades y funciones en el ENS, será la persona titular del órgano directivo que tiene la responsabilidad última del uso que se haga de la información y, por tanto, de su protección. Coincidirá con la figura de responsable del tratamiento que se define en el artículo 4 del RGPD

salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa.

3. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de este perfil de responsabilidad, dentro de su ámbito de actuación y sin perjuicio de otras previstas en el ENS y la guía CCN-STIC-801, son los siguientes:

a) Ayudar a determinar los requisitos de seguridad de la información, identificando los niveles de seguridad de dicha información mediante la valoración del impacto sobre esta de los incidentes que pudieran producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello, contará con la ayuda de la persona responsable del sistema.

c) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas que sean de su competencia.

4. El nombramiento o renovación de las personas responsables de la información se realizará en virtud de la presente política de seguridad TIC, y conservarán su condición mientras ostenten el cargo que haya determinado su nombramiento."

En el **apartado 1**, se aprecia una errata al referirse al Esquema Nacional de Seguridad, al que se denomina como *"Esquema Nacional de Seguridad y Salud"*.

En el **apartado 2**, se aconseja la sustitución de la segunda frase *"Coincidirá con la figura de responsable del tratamiento que se define en el artículo 4 del RGPD salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa",* por la siguiente:

"Tendrá la consideración de responsable del tratamiento definida en el artículo 4 del RGPD el órgano directivo cuya persona titular ostente la condición de responsable de la información, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan otra cosa."

Todo ello porque como se indica en las Directrices 07/2020 del CEPD, adoptada el 7 de julio de 2021, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, si bien en principio no existen restricciones en relación con el tipo de ente que puede asumir la función

de responsable del tratamiento, en la práctica suele tratarse de la propia organización como tal, y no de una persona dentro de ésta.

En conexión con esto último, se recomienda igualmente sustituir en todo el texto del proyecto de Orden la expresión "*la persona responsable del tratamiento*" por la de "*el responsable del tratamiento*" al referirse a un órgano directivo.

En el **apartado 3**, se sugiere introducir una letra d) en la que figuren, en consonancia con lo dispuesto en el RGPD, las obligaciones del responsable de la información relativas a los análisis de riesgos en materia de protección de datos, en cuanto responsable del tratamiento, con la siguiente redacción:

"Impulsar la adopción de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, cumplir con las obligaciones establecidas en el artículo 38 de la presente Orden, relativo a la evaluación de impacto."

14. Sobre el "artículo 19. Unidad de Seguridad Interior."

El art. 19 del proyecto de Orden establece:

"De conformidad con lo dispuesto en el artículo 10 del Decreto 171/2020, de 13 de octubre, la Consejería de Universidad, Investigación e Innovación contará con una Unidad de Seguridad Interior, la cual ejercerá la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito.

La Unidad de Seguridad Interior de la Consejería de Universidad, Investigación e Innovación tendrá las siguientes funciones:

a) Realizar las labores de soporte, asesoramiento e información al Comité de Seguridad Interior y Seguridad TIC, así como la ejecución de sus decisiones y acuerdos en materia de seguridad interior y la propuesta de un Plan de Seguridad Interior para la Consejería.

b) Proponer las adaptaciones necesarias a su ámbito del modelo general de seguridad interior, incluso valores, tablas y métricas adecuadas al conjunto de los activos en su ámbito.

c) Realizar el desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior en la Consejería.

d) Llevar a cabo la generación y supervisión de criterios y directrices para la gestión de la seguridad interior en el ámbito de la Consejería.

e) Realizar la recogida sistemática de información y la supervisión del estado de las principales variables de seguridad interior en el ámbito de la Consejería.

f) Realizar la coordinación y el seguimiento de la actividad de los puntos coordinadores responsables de seguridad interior de la Consejería.

g) Realizar el asesoramiento técnico y la auditoría del sistema de seguridad interior en el ámbito de la Consejería.

h) Velar por la coherencia de la aplicación del modelo de seguridad interior en el ámbito de la Consejería, mantenerlo actualizado e impulsar su implantación.

i) Gestionar para el ámbito de la Consejería o entidad, la relación con la Unidad Corporativa de Seguridad Interior.

j) Definir los criterios de protección de activos especialmente sensibles a riesgos que conciernen a la seguridad interior conforme a las especificidades del ámbito de la Consejería.

k) Desarrollar para el ámbito de la Consejería, planes de contingencia en respuesta a incidentes de seguridad interior, incluso situaciones de crisis.

l) Asegurar en el ámbito de la Consejería, el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto.

m) Promover y coordinar la cooperación con las autoridades del sector correspondiente al ámbito material de la Consejería en materia de inteligencia para la seguridad.

n) Informar sobre incidentes de seguridad interior en la Consejería que se consideren relevantes.

ñ) Asegurar en su nivel el correcto funcionamiento en la cadena de comunicación y escalado de incidentes de seguridad interior.

o) Proponer a la aprobación del Comité de Seguridad Interior y Seguridad TIC el Plan de Seguridad Interior de la Consejería o entidad dependiente singular.

p) Cuantas otras le sean encomendadas en relación con la seguridad interior por el Comité de Seguridad Interior y Seguridad TIC.

2. El nombramiento y cese de las personas responsables y aquellas que componen las Unidades de Seguridad Interior de la Consejería de Universidad, Investigación e Innovación , se llevará a cabo por el Comité de Seguridad Interior y de Seguridad TIC de la Consejería. El nombramiento y cese será comunicado a dichas personas afectadas."

Este precepto tiene dos apartados, sin embargo, al comienzo del precepto no figura el número 1 correspondiente al primer apartado. Se propone que el mismo comience así: "1. De conformidad…".

En el **apartado 1**, sobre las funciones de dicha Unidad, **letra a)**, se aconseja la supresión del inciso final: "*propuesta de un Plan de Seguridad Interior para la Consejería*", por estar fuera del contexto de las funciones enumeradas en la misma, y concretarse, posteriormente, de forma expresa la propuesta de dicho Plan en letra o) del apartado 1.

En el **apartado 1 letra l)**, **en** la medida en que los mecanismos citados en el mismo impliquen un tratamiento de datos personales, deberá explicitarse el mismo, recoger sus elementos principales y determinar las medidas técnicas y organizativas adecuadas para garantizar el cumplimiento en materia de protección de datos.

15. Sobre el "artículo 20. Unidad de Seguridad TIC."

El art. 20 del proyecto de Orden indica:

"*1. En virtud de lo establecido en el artículo 11.1 del Decreto 1/2011, de 11 de enero, la Consejería de Universidad, Investigación e Innovación contará con una Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho decreto.*

La Unidad de Seguridad TIC de la Consejería de la Consejería de Universidad, Investigación e Innovación tendrá las atribuciones que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero, que se indican a continuación:

a) Las labores de soporte, asesoramiento e información al Comité de Seguridad Interior y de Seguridad TIC, así como de ejecución de las decisiones y acuerdos adoptados por este.

b) El diseño y ejecución de los programas de actuación propios, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, auditorías de cumplimiento y planes de adecuación legal.

c) La definición, implantación y mantenimiento de los controles de carácter organizativo para la protección delos datos, aplicaciones y sistemas, así como la realización y mantenimiento de los análisis de riesgos.

d) La supervisión sistemática de los controles de carácter procedimental, operacional y de las medidas técnicas de protección de los datos, las aplicaciones y los sistemas.

e) La definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al centro o centros directivos responsables de la información y del servicio.

f) La definición y ejecución de los programas formativos y de concienciación relacionados con las buenas prácticas de seguridad TIC, promoviendo, en el proceso de selección de las personas participantes en estos programas, la aplicación del principio de igualdad de género.

g*) La aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC corporativa.*

h) La elaboración y mantenimiento de un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad TIC.

2. La persona responsable de la Unidad de Seguridad TIC de la Consejería tendrá la condición de responsable de seguridad TIC.

3. El nombramiento y cese de las personas responsables y aquellas que componen las Unidades de Seguridad TIC de la Consejería de Universidad, Investigación e Innovación, se llevará a cabo por el Comité de Seguridad Interior y de Seguridad TIC de la Consejería. El nombramiento y cese será comunicado a dichas personas afectadas."

En el **apartado 1 letra c)** se propone incluir que las funciones detalladas en el mismo se desempeñarán con el asesoramiento del delegado de protección de datos, en sintonía con lo indicado en el artículo 3.2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y con el contenido de los requisitos de protección de la información sobre datos personales contemplado en el apartado 5.7.1 del Anexo II de dicho Real Decreto.

En el **apartado 1 letra e)** se recomienda que para la definición y supervisión de los criterios y requisitos técnicos de seguridad, se cuente asimismo con el asesoramiento del delegado de protección de datos, para contemplar la protección de datos personales desde el diseño, de acuerdo con lo establecido en el artículo 25 del RGPD. Por ello, se sugiere que la primera frase del art. 20.1.e) quede redactada así:

"e) La definición y supervisión de los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC, para lo que deberá contar con el asesoramiento del delegado de protección de datos."

16. Sobre el "artículo 21. Responsable de seguridad TIC."

El art. 21 del proyecto de Orden dice:

"*1. La persona responsable de seguridad TIC será la encargada de velar por la armonización de la seguridad de la información en sus diferentes vertientes, y tendrá las siguientes funciones y responsabilidades:*

a) Dirigirá la Unidad de Seguridad TIC de la Consejería de Universidad, Investigación e Innovación.

b) Elaborará la normativa de seguridad que se presentará al Comité de Seguridad Interior y Seguridad TIC para su aprobación.

c) Será responsable de:

1.º Conocer los cambios tecnológicos que puedan afectar a los sistemas de información, pudiendo tener consecuencias para la organización. En este caso deberá alertar al Comité de Seguridad Interior y Seguridad TIC y proponer las medidas oportunas.

2.º La correcta ejecución de las instrucciones emanadas del Comité de Seguridad Interior y Seguridad TIC, transmitiendo dichas instrucciones directamente o a través de la Unidad de Seguridad TIC.

3.º La presentación regular de informes sobre el estado de seguridad de los servicios TIC al Comité de Seguridad Interior y Seguridad TIC.

4.º La preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres.

5.º La elaboración del Análisis de Riesgos de los sistemas, análisis que será presentado al Comité de Seguridad Interior y Seguridad TIC para su aprobación. Este análisis deberá actualizarse regularmente dependiendo de la criticidad del sistema.

6.º La inspección de las verificaciones regulares de seguridad aprobadas por el Comité. El resultado de estas inspecciones se presentará al Comité de Seguridad Interior y Seguridad TIC para su conocimiento y aprobación. Si como resultado de la inspección aparecen incumplimientos, propondrá medidas correctoras que presentará al Comité de Seguridad Interior y Seguridad TIC para su aprobación, responsabilizándose de que sean llevadas a cabo.

7.º La elaboración y seguimiento del Plan de Seguridad que será presentado al Comité de Seguridad Interior y Seguridad TIC para su aprobación.

d) Determinará, para su aprobación por el Comité de Seguridad Interior y Seguridad TIC, los requisitos de formación y calificación de las personas con perfiles de personas administradoras, operadoras y usuarias desde el punto de vista de la seguridad de las TIC.

2. La persona responsable de seguridad TIC deberá poseer conocimientos de la normativa vigente y estándares nacionales e internacionales en seguridad de la información y de protección de datos, y, será nombrada entre el personal funcionario de la Unidad de Seguridad TIC por el Comité de Seguridad Interior y Seguridad TIC, mediante acto documentado."

Se propone la siguiente redacción para el **apartado 1, letra c) número 5º**, con el fin de contar con el asesoramiento del delegado de protección de datos en los análisis de riesgos:

"5.º La elaboración del Análisis de Riesgos de los sistemas, contando con el asesoramiento del delegado de protección de datos. Dicho análisis será presentado al Comité de Seguridad Interior y Seguridad TIC para su aprobación. Este análisis deberá actualizarse regularmente dependiendo de la criticidad del sistema."

17. Sobre el "artículo 25. Gestión de riesgos."

El art. 25 del proyecto de Orden dispone:

"1. La Consejería de Universidad, Investigación e Innovación realizará una gestión de la seguridad basada en los riesgos, propiciando que tanto el análisis como la gestión de riesgos sean parte esencial del proceso de seguridad, que deberá ser lo más transversal posible al resto de procesos de la organización.

2. La gestión de riesgos deberá realizarse de manera continua sobre cada sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y evaluación periódica. Dicha gestión permitirá mantener un entorno controlado, minimizando los riesgos hasta niveles aceptables, reduciendo estos niveles mediante el despliegue de medidas de seguridad, proceso para el que se establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

3. El proceso de gestión de riesgos comprende las fases de identificación y valoración de las informaciones y los servicios esenciales prestados, la categorización de los sistemas, el análisis de riesgos y la selección de las medidas de seguridad a aplicar, las cuales deberán estar justificadas y ser proporcionales a los riesgos."

Se propone incluir un **nuevo párrafo final del apartado 1,** en conexión con el artículo 3.2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, indicando lo siguiente:

"En los supuestos de sistemas de información que traten datos personales, 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."

18. Sobre el "artículo 26. Responsabilidades en la gestión de riesgos."

El art. 26 del proyecto de Orden establece:

"*1. Las personas responsables de la información y/o responsables del servicio serán responsables de los riesgos sobre la información y/o los servicios respectivamente y, por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.*

2. El Comité de Seguridad Interior y Seguridad TIC será responsable de realizar un seguimiento de los principales riesgos residuales asumidos por la organización y de recomendar posibles actuaciones respecto de ellos.

3. La selección de las medidas de seguridad a aplicar será propuesta por la Unidad de Seguridad TIC al Comité de Seguridad Interior y Seguridad TIC, así como el seguimiento de su aplicación."

Se recomienda introducir un **nuevo apartado,** entre los actuales apartados primero y segundo, relativo a la responsabilidad en la gestión de riesgos en los tratamientos de datos personales, del tenor siguiente:

"El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, será responsable de analizar los riesgos para los derechos y libertades de las personas físicas que conlleven los tratamientos de datos personales de los que sea responsable y aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo."

19. Sobre el "artículo 30. Gestión de incidentes de seguridad y de la continuidad."

El art. 30 del proyecto de Orden señala:

"*1. El Comité de Seguridad Interior y Seguridad TIC deberá aprobar y revisar periódicamente un plan para mantener la continuidad de los procesos y sistemas críticos y garantizar su recuperación en caso de desastre. La finalidad de este plan es reducir el tiempo de indisponibilidad a niveles aceptables mediante la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.*

2. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la administración, el sector empresarial y la ciudadanía de la Comunidad Autónoma de Andalucía (en adelante, AndalucíaCERT).

3. En relación con la violación de la seguridad de los datos personales, se actuará de acuerdo con lo previsto en el artículo 40."

Para valorar si un incidente de seguridad afecta a datos personales, se sugiere modificar el **apartado 3**, que debería tener la siguiente redacción:

"3. Durante la gestión de los incidentes de seguridad se analizará si han sido afectados datos personales, en cuyo caso se actuará de acuerdo con lo previsto en el artículo 40 de la presente Orden, relativo a la violación de la seguridad de los datos personales."

20. Sobre el "artículo 31. Concienciación y formación. Obligaciones del personal."

El art. 31 del proyecto de Orden indica:

"*1. La seguridad de la información afecta a todas las personas que prestan servicios en la Consejería de Universidad, Investigación e Innovación y a todas las actividades, de acuerdo con el principio de seguridad integral recogido en el artículo 5 del Real Decreto 4/2010, de 8 de enero. El objetivo consiste en lograr la*

plena conciencia de estas personas, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que pueden acaecer. Adicionalmente, las personas con responsabilidad en el uso, operación y administración de sistemas TIC deberán haber recibido formación en el manejo seguro de los sistemas, en la medida en que la necesiten para realizar sus funciones.

2. Todas las personas que presten sus servicios en la Consejería de Universidad, Investigación e Innovación tienen la obligación de conocer y cumplir esta política de seguridad TIC y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

3. Todo el personal de la Consejería de Universidad, Investigación e Innovación estará obligado a asistir a un curso o sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todas las personas pertenecientes a la Consejería de Universidad, Investigación e Innovación, en particular a aquellas de nueva incorporación."

En la **primera frase del apartado 1** se recomienda hacer referencia al principio de seguridad como proceso integral, consagrado en el artículo 6 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en lugar de la mención realizada al Real Decreto 4/2010, de 8 de enero que, por otra parte y en todo caso, debía entenderse referida al Real Decreto 3/2010, de 8 de enero, que es el que regulaba, en su artículo 5, la seguridad como un proceso integral.

21. Sobre el "artículo 32. Terceras partes."

El art. 32 del proyecto de Orden dice:

"*1. Cuando la Consejería de Universidad, Investigación e Innovación preste servicios a otras entidades o departamentos, o maneje información de estos, se les hará partícipes de esta política de seguridad TIC, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad Interior y Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.*

2. Cuando la Consejería de Universidad, Investigación e Innovación utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que ataña a estos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias, así como se garantizará

que el personal correspondiente a dicha tercera parte esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC.

3. Cuando algún aspecto de la política de seguridad TIC no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, la persona responsable de seguridad TIC requerirá un informe que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por la persona responsable de la información y la persona responsable del servicio afectados antes de continuar con las actuaciones."

En el **apartado 1**, en cumplimiento de lo establecido en el artículo 28 del RGPD, se recomienda incluir una referencia a las violaciones de seguridad de los datos personales como parte de los procedimientos de actuación. De esa forma el **inciso final del apartado 1** quedaría redactado de la siguiente forma:

"...y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad y violaciones de seguridad de los datos personales."

En la misma línea, se sugiere el siguiente cambio en la redacción de la **última frase del apartado 2**:

"[...] Se establecerán procedimientos específicos de comunicación y resolución de incidencias, y violaciones de seguridad de los datos personales, así como se garantizará que el personal correspondiente [...]"

Asimismo, en el **apartado 2** se propone incluir una mención al deber de confidencialidad al que también se encuentran sometidos los terceros cuyos servicios sean utilizados por la Consejería o a los que ésta les ceda o comunique información, según se infiere de lo dispuesto en el artículo 5.1 de la LOPDGDD en relación con el artículo 5.1.f) del RGPD.

22. Sobre el "artículo 33. Auditorías y conformidad normativa."

El art. 33 del proyecto de Orden dispone:

"*1. La Consejería de Universidad, Investigación e Innovación manifiesta el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente.*

2. Los sistemas de información de la Consejería de Universidad, Investigación e Innovación serán objeto, al menos, cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La

Unidad de Seguridad TIC coordinará estas actividades de auditoría, y analizará y elevará a la persona responsable de seguridad TIC, a la persona responsable del sistema y a la persona delegada de protección de datos si las conclusiones afectan a los datos de carácter personal. La persona responsable del sistema adoptará las medidas correctoras adecuadas. Si las conclusiones requieren, a priori, un cambio normativo, deberán elevarse al Comité de Seguridad Interior y Seguridad TIC para que adopte las medidas adecuadas.

3. Con carácter extraordinario deberán realizarse auditorías siempre que se produzcan modificaciones sustanciales en el sistema de información con un potencial impacto en el cumplimiento de las medidas de seguridad.

4. Los informes de auditoría quedarán a disposición de la persona titular de la Consejería y del Comité de Seguridad Interior y Seguridad TIC."

Se sugiere incluir expresamente en este precepto la realización de auditorías sobre el cumplimiento en materia de protección de datos, en aquellos sistemas de información que traten datos personales.

En el **apartado 2,** se sugiere incluir las funciones que realizará el delegado de protección de datos en el caso de que las conclusiones afectan a datos personales.

Además, en el **apartado 2** sería recomendable revisar la redacción de la segunda frase: "*La Unidad de Seguridad TIC coordinará estas actividades de auditoría, y analizará y elevará a la persona responsable de seguridad TIC, a la persona responsable del sistema y a la persona delegada de protección*[...]" en aras a una mayor claridad. Y la referencia "*a la persona delegada de protección de datos*" debería sustituirse por la de "*al delegado de protección de datos*", pues la figura del delegado de protección de datos puede ser atribuida a un grupo de personas y, de esta forma, no se prejuzga la forma de cubrir este puesto.

23. Sobre el "artículo 37. Incidencia de la normativa de protección de datos de carácter personal."

El art. 37 del proyecto de Orden establece:

"*1. Todos los sistemas de información de la Consejería se ajustarán a lo exigido por el RGPD, y por el resto de la normativa general o sectorial de protección de datos de carácter personal que sea de aplicación. Todos los tratamientos de datos de carácter personal, automatizados o no automatizados, se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación. En dicho ámbito cada responsable del tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son confor-*

mes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del RGPD.

2. Las medidas técnicas y organizativas a implantar tendrán en cuenta lo previsto en el artículo 13.h) de la Ley 39/2015, de 1 de octubre, que reconoce como derecho de toda la ciudadanía ante las Administraciones Públicas en sus relaciones con ella la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

3. Las personas responsables del tratamiento en el ámbito de aplicación de esta orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo."

En el **apartado 1** se recomienda incluir, de forma expresa, los sistemas de información de las entidades vinculadas o dependientes de la Consejería.

Además, se sugiere incluir en la **primera frase del apartado 1,** después de la referencia al "RGPD", una mención expresa a la LOPDGDD (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), que se habrá mencionado en el texto de la Orden si se atiende el comentario referido al artículo 3 del proyecto de Orden (apartado IV.4 de esta informe).

En consonancia con lo anterior, en la **segunda frase del apartado 1**, se sugiere sustituir la expresión *"se sujetarán a la citada norma cuando se encuentren dentro de su ámbito de aplicación"* por la de "se sujetarán a la citada normativa cuando se encuentren dentro de su ámbito de aplicación*",* para hacer referencia a toda la normativa vigente en materia de protección de datos y no únicamente al RGPD.

Igualmente, en el **inciso final de la tercera frase del apartado 1**, se propone la siguiente redacción, con el fin de mencionar expresamente el artículo 5.2 del RGPD cuando se alude al principio de responsabilidad proactiva: "(...),de acuerdo con el principio de responsabilidad proactiva, previsto en el artículo 5.2 del RGPD, y de conformidad con el artículo 24 del RGPD."

Por tanto, atendiendo a las cuatro recomendaciones anteriores, la redacción del **apartado 1** quedaría con el siguiente tenor literal:

"1. Todos los sistemas de información de la Consejería y sus entidades vinculadas o dependientes se ajustarán a lo exigido por el RGPD, por la LOPDGDD y por el resto de la normativa general o sectorial de protección de datos personales que sea de aplicación. Todos los tratamientos de datos personales, automatizados o no automatizados, se sujetarán a la citada normativa cuando se encuentren dentro de su ámbito de aplicación. En dicho ámbito, cada responsable del tratamiento de datos per-

sonales aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos personales son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva previsto en el artículo 5.2 del RGPD, y de conformidad con el artículo 24 del RGPD."

Asimismo, en el **apartado 2** se sugiere sustituir la expresión "...*que reconoce como derecho de toda la ciudadanía ante las Administraciones Públicas en sus relaciones con ella la protección de datos de carácter personal*..." por *"...* que reconoce a las personas, en sus relaciones con las Administraciones Públicas, el derecho a la protección de datos personales*..."* por estimarse más ajustada a lo establecido en el citado artículo 13. letra h) de la Ley 39/2015 y al RGPD.

Además, se recomienda modificar la redacción del **final del apartado 3** para aclarar que en el ámbito de la protección de datos se debe atender a los riesgos para los derechos y libertades de las personas físicas, así como realizar revisiones periódicas de las medidas adoptadas, proponiéndose la siguiente redacción: "[...] *aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas, que serán revisadas regularmente, de conformidad con el artículo 32 del RGPD.*"

Por último, se sugiere introducir un nuevo **apartado 4** que haga alusión al principio de confidencialidad previsto en el artículo 5.1 f) del RGPD, al que están sujeto todas las personas, físicas o jurídicas, que actúen bajo la autoridad del responsable de un tratamiento, de conformidad con lo previsto en el artículo 5.1 de la LOPDGDD, así como mencionar que tal deber se extiende aún después de finalizada la relación del obligado con dicho responsable del tratamiento, de acuerdo con el artículo 5.3 de la citada Ley.

24. Sobre el "artículo 39. Registro de actividades de tratamiento."

El art. 39 del proyecto de Orden indica:

"*1. El responsable del tratamiento llevará un registro de las actividades de tratamiento de datos personales efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el resto de normativa de datos personales aplicable. Los responsables del tratamiento harán públicas y mantendrán actualizadas sus actividades de tratamiento en el inventario de actividades de tratamiento de datos de la Junta de Andalucía.*

2. Cada persona encargada del tratamiento llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable, de conformidad con lo previsto en aquel artículo.

3. Los responsables o encargados del tratamiento deberán comunicar a la persona Delegada de Protección de Datos, cualquier adición, modificación o exclusión en el contenido del registro en virtud de lo establecido en el artículo 31.1, párrafo tercero, de la Ley Orgánica 3/2018, de 5 de diciembre."

Se recomienda iniciar el **apartado 1** con la expresión "Cada responsable de tratamiento …".

25. Sobre el "artículo 40. Violación de la seguridad de los datos personales."

El art. 40 del proyecto de Orden señala:

"*1. En caso de violación de la seguridad de los datos personales, la persona responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, con un plazo máximo de 72 horas posteriores a computar desde que haya tenido constancia de ella, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en dicho plazo máximo, esta deberá ir acompañada de la indicación de los motivos de la dilación. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. Dicha notificación y comunicación se atendrán a lo establecido en los artículos 33 y 34 del RGPD y en el resto de la normativa de datos de carácter personal aplicable.*

2. La notificación a la autoridad de control a la que se refiere el apartado anterior se realizará a través del formulario elaborado por el Consejo de Transparencia y Protección de Datos para las notificaciones de violaciones de seguridad que, dentro de su ámbito competencial, hayan de serle notificadas por parte de los responsables de tratamiento, una vez finalizado el protocolo de actuación establecido por la Consejería."

En relación al **principio del apartado 1**, debe recordarse que la autoridad de control competente es el Consejo de Transparencia y Protección de Datos de Andalucía. Por otra parte, se sugiere indicar expresamente la necesidad de valorar los riesgos de la violación de la seguridad, por parte del responsable del tratamiento. Por ello, se propone la siguiente redacción, en aras a su clarificación:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento lo pondrá en conocimiento del delegado o delegada de protección de datos, efectuará la valoración del riesgo que la misma suponga para los derechos y libertades de las personas físicas, y la notificará al Consejo de Transparencia y Protección de Datos de Andalucía sin dilación indebida…"

Para completar las obligaciones del responsable del tratamiento respecto a las violaciones de la seguridad de los datos personales, se propone añadir al **final** de la actual redacción del **apartado 1**, la si-

guiente frase: "[...]En todo caso, el responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.".

Se sugiere eliminar el **inciso final del apartado 2:** "*una vez finalizado el protocolo de actuación establecido por la Consejería*", dado que la obligación de notificar al Consejo de Transparencia y Protección de Datos de Andalucía nace en el mismo momento en que se tiene conocimiento de la violación de la seguridad de los datos personales, y debe realizarse sin dilación indebida, con independencia de que haya concluido el proceso de resolución de la misma. En caso de no disponer de toda la información simultáneamente, ésta se facilitará de manera gradual, sin dilación indebida, mediante las notificaciones complementarias que fuesen necesarias, conforme al art. 33.4 del RGPD.

26. Sobre el "artículo 41. Persona delegada de protección de datos."

El art. 41 del proyecto de Orden dice:

"*1. La figura de delegado de protección de datos será designada atendiendo a sus cualidades profesionales, en particular deberá tener un perfil jurídico especializado y práctica en materia de protección de datos, de conformidad con lo establecido en los artículos 37 y 38 del RGPD y los artículos 34 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre.*

2. El delegado de protección de datos no recibirá 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, salvo que incurriera en dolo o negligencia grave en su ejercicio.

3. La designación, nombramiento y cese del delegado de protección de datos deberá comunicarse en el plazo de diez días al Consejo de Transparencia y Protección de Datos de Andalucía."

En el **título de este artículo** debería sustituirse la referencia "*persona delegada de protección de datos*" por la de "*delegado de protección de datos*", tal y como se ha indicado en el apartado IV. 22 de este informe, pues la figura del delegado de protección de datos puede ser atribuida a un grupo de personas y, de esta forma, no se prejuzga la forma de cubrir este puesto.

En consonancia con lo dispuesto en los artículos 37 del RGPD y 35 de la LOPDGDD, se propone la siguiente redacción del **apartado 1**: "El delegado de protección de datos será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, de conformidad con lo establecido en los artículos 37 del

RGPD y 35 de la LOPDGDD. En la designación deberá especificarse el alcance de la misma, indicando los responsables de tratamiento para los que ejercerá sus funciones".

En la **primera frase del apartado 2** se sugiere incluir la mención al responsable y encargado del tratamiento, en lo referido a la imposibilidad de dictar instrucciones, de acuerdo con lo previsto en el art. 38.3 del RGPD.

27. Sobre el "artículo 42. Persona delegada de protección de datos en las entidades vinculadas o dependientes."

El art. 42 del proyecto de Orden dispone:

"*La dirección de cada entidad vinculada o dependiente deberá nombrar una persona delegada de protección de datos que se comunicará a la Agencia Española de Protección de Datos y al Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación. La persona delegada de protección de datos, que deberá estar en posesión de una titulación superior, será designada atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de Derecho y la práctica en materia de protección de datos, de conformidad con el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre.*"

Sin perjuicio de lo que se indicará en el párrafo siguiente, en el **título de este artículo** debería sustituirse la referencia "*persona delegada de protección de datos*" por la de "*delegado de protección de datos*", tal y como se ha indicado en el apartado IV. 22 y 26 de este informe, pues la figura del delegado de protección de datos puede ser atribuida a un grupo de personas y, de esta forma, no se prejuzga la forma de cubrir este puesto.

Además, con el fin de dotar de mayor coherencia al texto, se propone que este artículo tenga una redacción similar a la forma en que finalmente se redacte el art. 41 del proyecto de Orden, relativo a la persona delegada de protección de datos o, mejor aún, unificar ambos artículos en uno solo.

En cualquier caso, en la **primera frase**, debe sustituirse la referencia a la Agencia Española de Protección de Datos por la del Consejo de Transparencia y Protección de Datos de Andalucía, como autoridad de control competente en la Comunidad Autónoma de Andalucía.

28. Sobre el "artículo 43. Responsables del tratamiento de datos de carácter personal."

El art. 43 del proyecto de Orden establece:

"*1. Las personas responsables del tratamiento de datos de carácter personal en el ámbito de aplicación de esta orden son las autoridades públicas que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.*

2. En el ámbito de la política de seguridad TIC de la Consejería de Universidad, Investigación e Innovación, las personas responsables de la información tendrán la condición de responsables del tratamiento respecto a los tratamientos sobre los que determinen sus fines y medios, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos de carácter personal dispongan otra cosa."

En el **título de este artículo** deberían eliminarse las palabras "*de datos de carácter personal*", para ajustar el encabezamiento de este artículo a la denominación utilizada en el RGPD (ver su art. 4.7).

En concordancia con el comentario realizado sobre el artículo 17 del proyecto de Orden, relativo al responsable de la información (ver apartado IV. 13 de este informe), se recomienda la siguiente redacción para el **apartado 1:**

"1. Los responsables del tratamiento en el ámbito de aplicación de esta orden son los órganos directivos que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD."

Por otra parte, para evitar duplicidades en el texto, se sugiere eliminar totalmente el **apartado 2,** por ya estar contenido en el artículo 17 del proyecto de Orden, relativo al responsable de la información.

29. Sobre el "artículo 44. Personas encargadas del tratamiento de datos de carácter personal."

El art. 44 del proyecto de Orden señala:

"*1. De conformidad con el artículo 28 del RGPD cuando se vayan a tratar datos personales por cuenta de un responsable, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, y garantice la protección de los derechos de las personas interesadas. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico constará por escrito, inclusive en formato electrónico.*

2. Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del RGPD y demás normativa de aplicación.

3. El encargado del tratamiento, y cualquier persona que actúe bajo la autoridad de la persona responsable o encargada del tratamiento, y tenga acceso a datos personales, solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud de normativa aplicable."

En el **título de este artículo** debería sustituirse su denominación actual "*personas encargadas del tratamiento de datos de carácter personal*", por la de "encargados del tratamiento", por ser la denominación utilizada en el RGPD (ver su art. 4.8).

En el **inciso final de la primera frase del apartado 1** se sugiere sustituir la expresión *"... y garantice la protección de los derechos de las personas interesadas."* por "... de manera que el tratamiento garantice la protección de los derechos del interesado.", haciéndolo concordar con el artículo 28.1 del RGPD.

Se propone una ligera modificación del **apartado 3**, con el fin de incidir en la obligación de que el encargado trate los datos personales siguiendo instrucciones documentadas del responsable, tal y como se establece en el artículo 28.3 a) del RGPD. La redacción del mismo sería, pues, la siguiente:

"3. El encargado del tratamiento, y cualquier persona que actúe bajo la autoridad de la persona responsable o encargada del tratamiento, y tenga acceso a datos personales, solo podrán tratar dichos datos siguiendo instrucciones **documentadas** del responsable, a no ser que estén obligados a ello en virtud de normativa aplicable."

30. Sobre la inclusión de un nuevo artículo sobre "Concienciación, formación y obligaciones del personal en materia de protección de datos".

Se sugiere introducir en el proyecto de Orden un artículo concreto que regule la "Concienciación, formación y obligaciones del personal en materia de protección de datos" o, en su defecto, que se incluya esta cuestión, como un apartado específico en el artículo 31 del proyecto de Orden, relativo a la "Concienciación y formación. Obligaciones del personal".

31. Consideración final, de carácter general.

Mas allá de las cuestiones específicas que se han señalado en el presente informe, se recuerda que esta Comisión Consultiva ya se ha pronunciado, en otras ocasiones, sobre la necesidad de que la Administración de la Junta de Andalucía mantenga un criterio uniforme a la hora de regular las políticas de seguridad en las distintas Consejerías, tal y como se desprende del espíritu del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Aunque cada organización, en su orden interno, pueda establecer su propia estructura organizativa, debe garantizarse la existencia de elementos comunes en la Administración de la Junta de Andalucía , para evitar incoherencias en cuestiones que son relevantes desde la óptica de la normativa de protección de datos, tales como el rol que debe desempeñar el delegado de protección de datos en materia de seguridad o la definición de la figura de responsable del tratamiento.

Es todo cuanto cabe señalar respecto del proyecto de norma en tramitación.

El presidente de la Comisión
Consta la firma
Jesús Jiménez López