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 POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA CONSEJERÍA DE TURISMO, CULTURA Y DEPORTE

I.- Con fecha 17 de mayo de 2023 ha tenido entrada en el Consejo de Transparencia y Protección de Datos de Andalucía solicitud de informe, efectuada por la Consejería de Turismo, Cultura y Deporte, referente al proyecto de Orden por la que se aprueba la Política de Seguridad de la Consejería de Turismo, Cultura y Deporte.

Con la petición de informe se acompaña el proyecto de Orden citado y se facilita un enlace, a consigna de la Junta de Andalucía, para acceder al resto de documentación que conforma el expediente.

II.- La Comisión Consultiva de la Transparencia y la Protección de Datos de Andalucía 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. Cambio en el título de la norma.

Se sugiere que en el título de la propia Orden se sustituya la palabra *"aprueba"* por la de "*establece"*, en consonancia con la denominación 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 así como el 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, y de las diversas Órdenes que sobre la materia se han publicado en el ámbito de las Consejerías de la Junta de Andalucía (entre otras, Orden de 21 de octubre de 2019, de la Consejería de Hacienda, Industria y Energía, Orden de 3 de diciembre de 2020, de la Consejería de Educación y Deporte, Orden de 31 de agosto de 2020, de la Consejería de Empleo, Formación y Trabajo Autónomo).

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 la Exposición de Motivos.

A. Cuarto párrafo.

El **cuarto párrafo** de la **Exposición de Motivos** del proyecto de Orden indica:

"*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) dispone que todo tratamiento de datos personales que se lleve a cabo en el ámbito de competencias de la Consejería se debe llevar a cabo atendiendo al principio de responsabilidad proactiva que, entre otras implicaciones, incluye la necesidad de que el responsable adopte medidas técnicas y organizativas para garantizar la seguridad de los tratamientos de datos personales*."

Se aconseja que el **inciso final** del **cuarto párrafo** tenga la siguiente redacción (se subraya lo que se añade): "*... para garantizar la seguridad <u>adecuada al riesgo</u> de los tratamientos de datos personales*". La redacción propuesta permite reflejar, convenientemente, lo dispuesto en el artículo 32.1 primer párrafo, inciso final, del RGPD.

B. Noveno párrafo.

El **noveno párrafo** de la **Exposición de Motivos** del proyecto de Orden dice:

"*El artículo 12 de dicho Real Decreto exige cada Administración Pública dispongan de una política de seguridad formalmente aprobada por el órgano competente; la cual deberá estar basada en los principios básicos recogidos en el artículo 5 de la mencionada norma*." (Este párrafo alude al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad).

Se propone retocar la redacción del **noveno párrafo**, con el fin de ajustar su contenido al de la norma invocada (artículo 12 del Real Decreto 311/2022) así como corregir una errata gramatical, que tendría la siguiente redacción:

"*El artículo 12 de dicho Real Decreto exige que cada Administración Pública cuente con una política de seguridad formalmente aprobada por el órgano competente, la cual deberá establecerse de acuerdo con los principios básicos señalados en el capítulo II de la mencionada norma*".

4. Sobre el apartado 4 del artículo 3.

El **artículo 3** del proyecto de Orden, relativo a la responsabilidad general, dispone en su **apartado 4**:

"4. Cualquier persona física o jurídica que actúe bajo la autoridad del Responsable de un Tratamiento de datos personales en el ámbito de aplicación de la presente Orden y tenga acceso a datos personales, solo tratará dichos datos respetando las instrucciones del Responsable del Tratamiento, en cumplimiento del ordenamiento jurídico comunitario, nacional o autonómico."

En el **apartado 4** del **artículo 3** se sugiere hacer alusión al deber de confidencialidad previsto en el artículo 5.1 f) del RGPD en relación con el artículo 5 de la LOPDGDD, al que están sujetos las personas físicas o jurídicas que actúen bajo la autoridad del responsable de un tratamiento, así como mencionar que tal deber se extiende aún después de finalizada la relación del obligado con dicho responsable, tal y como expresamente señala el artículo 5.3 de la LOPDGDD.

5. Sobre el apartado 2 del artículo 4.

El **artículo 4** del proyecto de Orden, relativo a la estructura organizativa, establece en sus **apartados 1 y 2**:

"*1. La estructura organizativa de la política de seguridad de la Consejería estará compuesta por:*

a) El Comité de Seguridad Interior y Seguridad TIC (en adelante Comité de Seguridad), como órgano de definición, dirección y seguimiento de la política de seguridad de la Consejería.

b) Respecto a la ejecución de la política de seguridad interior:

1º Unidad de Seguridad Interior.

2º Puntos Coordinadores de Seguridad Interior.

3º Responsables de Seguridad de activos singulares, conjuntos u otros bienes singulares o conjunto de ellos, conforme a lo que se establezca en los instrumentos de planificación.

c) Respecto a la ejecución de la política de seguridad en el ámbito de las TIC:

1º Unidad de Seguridad TIC, cuya persona titular tendrá la condición de Responsable de Seguridad TIC.

2º Responsables de la Información.

3º Responsables del Servicio.

4º Responsables del Sistema.

d) Respecto a la ejecución de la política de seguridad en el ámbito de la protección de datos de carácter personal:

1º Delegado o Delegada de Protección de Datos.

2º Responsables del Tratamiento.

3º Encargados del Tratamiento.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrán recaer sobre una misma persona o grupo de personas, unidad o departamento.

No obstante, en todo caso, se deberá garantizar que la responsabilidad de la seguridad de las TIC esté diferenciada de la responsabilidad que es propia a la prestación de los servicios."

En el **apartado 2** del **artículo 4**, en relación con su **apartado 1, letra d), 2º**, se recuerda que las funciones del responsable del tratamiento también podrían recaer en un órgano administrativo, en la medida en que el artículo 5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, define los órganos administrativos indicando que: "*tendrán la consideración de órganos administrativos las unidades administrativas a las que se les atribuyan funciones que tengan efectos jurídicos frente a terceros, o cuya actuación tenga carácter preceptivo*".

6. Sobre el apartado 2 del artículo 6.

El **artículo 6** del proyecto de Orden, relativo a la naturaleza y composición del Comité de Seguridad Interior y Seguridad TIC, señala en su **apartado 2**:

"*2. El Comité de Seguridad estará formado por las siguientes personas:*

a) Presidencia: La persona titular de la Viceconsejería.

b) Vicepresidencia: La persona titular de la Secretaría General Técnica.

c) Vocalías:

1º La persona titular de cada uno de los órganos directivos de la Consejería que tenga responsabilidad sobre algún activo, tratamiento, información, servicio y/o sistema.

2º La persona titular de los órganos directivos de las entidades vinculadas o dependientes.

3º Las personas responsables de la Unidad de Seguridad TIC, de la Unidad de Seguridad Interior y la que ostente la condición de Delegado o Delegada de Protección de Datos.

4º Las personas titulares de las Coordinaciones Generales de la Viceconsejería y de la Secretaría General Técnica, que actuarán con voz, pero sin voto.

d) Secretaría: Recaerá en una persona funcionaria que ostente un puesto de nivel 28 o superior. Será designada por el propio Comité de Seguridad, que tendrá voz, pero no voto, que ejercerá las funciones propias de dicho cargo, entre otras convocar las reuniones por Orden de la persona titular de la presidencia, preparar el Orden del día y elaborar el acta de las sesiones. Esta función se ejercerá por un plazo máximo de cuatro años, prorrogables por otros cuatro."

En el **apartado 2, letra c), 3º**, se prevé la participación en el Comité de Seguridad, como vocal, de la persona que ostente la condición de Delegado o Delegada de Protección de Datos. Al respecto, debe advertirse que dicha participación debe producirse de forma que quede garantizada que sus funciones y cometidos no den lugar a conflicto de intereses, tal y como establece el art. 38. 6 del RGPD. Por ello, se propone que la persona que ostente la condición de Delegado o Delegada de Protección de Datos forme parte del Comité de Seguridad, con voz pero sin voto.

Además, se propone una nueva redacción del **apartado 2, letra d)**, en aras a su clarificación:

"*d) Secretaría: Recaerá en una persona funcionaria designada por el Comité de Seguridad que desempeñe un puesto de trabajo de nivel 28 o superior en la Consejería. Asistirá a las sesiones del Comité con voz pero sin voto y ejercerá las funciones propias de dicho cargo, entre otras, la de convocar las reuniones por orden de la persona titular de la presidencia, preparar el Orden del día de las mismas y elaborar el acta de las sesiones. Su designación será por un plazo máximo de cuatro años, prorrogable, una sola vez, por otros cuatro".*

7. Sobre el artículo 7. Funciones del Comité de Seguridad.

El **artículo 7** del proyecto de Orden, que regula las funciones del Comité de Seguridad, dice:

"Serán funciones propias del Comité de Seguridad:

a) Aprobar el desarrollo de la normativa de seguridad TIC, así como de las resoluciones que se aprueben por parte del órgano directivo central competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía, de conformidad con el artículo 2.5 de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

b) Establecer directrices comunes y de supervisión del cumplimiento de la normativa en materia de seguridad interior y seguridad TIC.

c) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad interior, incluido el Plan de Seguridad Interior, y de la seguridad TIC así como promover la dotación de recursos necesarios para el cumplimiento de dichas iniciativas y planes.

d) Velar para que todos los ámbitos de responsabilidad y actuación en relación con la política de seguridad queden perfectamente definidos, especialmente para asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades. Para ello, sin perjuicio de otras medidas, deberá aprobar el modelo de relación con los Puntos Coordinadores de Seguridad Interior.

e) Proporcionar, dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos a la Consejería, los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas. Entre ellas, la evaluación por parte de la Unidad de Seguridad TIC de los aspectos de seguridad de nuevos sistemas de información o de evolutivos de los existentes, antes de su puesta en producción, como se recoge en el apartado e) del artículo 11.1 del Decreto 1/2011, de 11 de enero.

f) Velar por el desarrollo, aprobación, implantación, y divulgación, así como por el cumplimiento y actualización del marco normativo y ejecutivo de seguridad interior, seguridad TIC y protección de datos de carácter personal en la Consejería.

g) Nombrar a los miembros de la Unidad de Seguridad Interior y a los miembros de la Unidad de Seguridad TIC de la Consejería, así como a las personas que asuman la responsabilidad de cada una de ellas. Igualmente nombrará a las personas responsables en materia de seguridad interior de las entidades adscritas a la Consejería.

Asimismo, le corresponderá nombrar a los Responsables del Sistema y a las personas que en las provincias asuman los Puntos Coordinadores de Seguridad.

h) Velar por la aplicación de la seguridad y protección de datos de carácter personal desde el diseño y, por defecto, en todos los nuevos proyectos o tratamientos de información que se pretendan llevar a cabo en la Consejería desde su concepción inicial. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

i) Promover, aprobar y realizar el seguimiento de la planificación de auditorías periódicas para verificar el correcto cumplimiento de la política, la normativa y los procedimientos de seguridad.

j) Aprobar las medidas correctoras que correspondan derivadas de las conclusiones elaboradas por la Unidad de Seguridad TIC, la Unidad de Seguridad Interior o por el Delegado o Delegada de protección de datos de carácter personal, a partir de su actividad o de los resultados de una auditoría.

k) Promover la formación y concienciación en materia de seguridad interior, seguridad TIC y de tratamiento diligente de datos personales entre el personal de la Consejería, así como la formación continua y especializada de los miembros de la Unidad de Seguridad Interior, de la Unidad de Seguridad TIC y del Delegado o Delegada de Protección de Datos.

l) Planificar y priorizar las iniciativas necesarias para cumplir con las directrices, los objetivos y los principios marcados en la política de seguridad regulada en la presente Orden. En especial, la elaboración, actualización y evaluación periódica de los análisis de riesgos necesarios.

m) Impulsar los preceptivos análisis de riesgos junto a la Unidad de Seguridad Interior, o la Unidad de Seguridad TIC y los perfiles Responsable de la Información, Responsable del Servicio y Delegado o Delegada de Protección de Datos. Para ello, se deberá impulsar la determinación de los niveles de seguridad de la información tratada y de los servicios prestados, usando la valoración de los impactos que tendrían los incidentes que afectaran a la política de seguridad.

n) Gestionar la aceptación de los riesgos residuales por sus responsables correspondientes respecto de la información y/o de los servicios de su competencia, obtenidos en el análisis de riesgos.

o) Monitorizar el desempeño del proceso de gestión de incidentes de seguridad, así como la toma de decisiones en respuesta a incidentes de seguridad críticos.

p) Establecer los mecanismos necesarios para compartir la documentación del marco regulador con el propósito de normalizarlo en todo el ámbito de aplicación y determinar los medios de difusión de la política de seguridad.

q) Establecer los mecanismos necesarios de coordinación de los diferentes órganos de seguridad de las entidades vinculadas o dependientes de la Consejería.

r) Proponer al Responsable de la Información las medidas técnicas y organizativas establecidas en la normativa de protección de datos de carácter personal, de acuerdo con los correspondientes análisis de riesgos y, en su caso, las evaluaciones de impacto en la protección de datos de carácter personal, contando con el asesoramiento del Delegado o Delegada de Protección de Datos.

s) Cuantas otras le sean encomendadas."

Se sugiere efectuar una pequeña modificación de la **letra f)** del **artículo 7** con el fin de hacer extensivas, de manera inequívoca, las funciones que en el mismo se contemplan, a los tres ámbitos mencionados en el artículo 1.1 del proyecto de Orden. Su redacción sería la siguiente:

"*f) Velar por el desarrollo, aprobación, implantación, divulgación, cumplimiento y actualización del marco normativo y ejecutivo en el ámbito de seguridad interior, seguridad TIC y protección de datos personales en la Consejería*".

En la **letra j)** del **artículo 7**, debe suprimirse la expresión *"de carácter personal",* de manera que la alusión sea al *"Delegado o Delegada de Protección de Datos",* sin más.

En la **letra k)**, sobre la promoción de la formación en determinadas materias, se aconseja sustituir la expresión *"...de tratamiento diligente de datos personales..."* por *"...en los principios relativos al tratamiento de datos personales...".*

Se sugiere sustituir la redacción de la **letra r)** del **artículo 7**, para ajustarla a lo dispuesto en el RGPD. Se propone la siguiente redacción:

"r) Proponer al Responsable del tratamiento las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad, 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 en la protección de datos personales, contando con el asesoramiento del Delegado o Delegada de Protección de Datos".

Asimismo, se recuerda la necesidad de que el responsable del tratamiento aplique las medias técnicas y organizativas apropiadas propuestas por el Comité de Seguridad así como que las mismas deben aplicarse desde el diseño y por defecto (art. 25 del RGPD).

8. Sobre los apartados 2 y 3 del artículo 8.

El **artículo 8** del proyecto de Orden, relativo al funcionamiento del Comité de Seguridad, establece en sus **apartados 2 y 3**:

"*2. El Comité de Seguridad podrá constituirse, convocar y celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como telemática, utilizando redes de comunicación a distancia, con las medidas adecuadas que garanticen la identidad de las personas comunicantes y la autenticidad de la información entre ellas transmitida.*

3. Cuando el tratamiento de determinadas cuestiones así lo requiera, se podrá convocar a las reuniones del Comité a personal técnico especializado, propio o externo, a los efectos de prestar asesoramiento experto, sin que en ningún caso pueda ocasionar coste económico."

Al objeto de reforzar las garantías de la información transmitida durante las actuaciones del Comité de Seguridad realizadas de forma telemática, se propone una nueva redacción del **inciso final** del **apartado 2**, que tendría la siguiente redacción: "*... 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 transmitida".*

Asimismo, con idéntico motivo, se propone añadir, a continuación, un nuevo párrafo (que sería el **segundo párrafo** del **apartado 2)** con el siguiente tenor: *"Las personas miembros del Comité de Seguridad están obligadas 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 técnico que pueda ser convocado a las reuniones del Comité, se aconseja completar la redacción del **apartado 3**, que quedaría como sigue:

"Cuando el tratamiento de determinadas cuestiones así lo requiera, se podrá convocar a las reuniones del Comité a personal técnico especializado, propio o externo, a los efectos de prestar asesoramiento experto, estando obligados a respetar la confidencialidad de toda la información a la que tengan acceso, sin que en ningún caso pueda ocasionar coste económico".

9. Sobre los apartados 2 y 4 del artículo 9.

A. Artículo 9 apartado 2.

El **artículo 9** del proyecto de Orden, que regula la Unidad de Seguridad Interior, dispone en su **apartado 2**, relativo a las funciones de la Unidad:

"2. Las funciones de la Unidad de Seguridad Interior, conforme a lo previsto en el artículo 10.2 Decreto 171/2020, de 13 de octubre, serán las siguientes:

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

d) Generar y supervisar los criterios y directrices para la gestión de la seguridad interior en el ámbito de esta Consejería.

e) Recoger de forma sistemática información y supervisar el estado de las principales variables de seguridad interior en el ámbito de esta Consejería.

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

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

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

i) Gestionar para el ámbito de la Consejería de Turismo, Cultura y Deporte , 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 de Turismo, Cultura y Deporte.

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

l) Asegurar en el ámbito de la Consejería de Turismo, Cultura y Deporte, 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 de Turismo, Cultura y Deporte en materia de inteligencia para la seguridad.

n) Informar sobre incidentes de seguridad interior en la Consejería de Turismo, Cultura y Deporte 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 el Plan de Seguridad Interior de la Consejería de Turismo, Cultura y Deporte dependiente singular.

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

En la **letra a)** del **apartado 2**, se aconseja la supresión de su **inciso final**, que dice: *"Propuesta de un Plan de Seguridad Interior para esta Consejería*", que parece ser una errata, por estar fuera del contexto del citado apartado, y estar expresamente prevista la propuesta de dicho Plan en la letra o) del apartado 2.

La **letra l)** del **apartado 2** recoge como función la de *"Asegurar en el ámbito de la Consejería de Turismo, Cultura y Deporte, 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*". En la medida en que dichos mecanismos impliquen un tratamiento de datos personales, deberá explicitarse el mismo, recoger sus elementos principales y determinar las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento en materia de protección de datos.

El **inciso final** de la **letra o)** del **apartado 2** "dependiente singular" parece un error que debería eliminarse.

B. Artículo 9 apartado 4.

El **artículo 9.4** del proyecto de Orden señala:

"4. A los efectos del adecuado cumplimiento de sus funciones, en la planificación de la seguridad interior se establecerán los mecanismos o instrumentos de comunicación inmediata y permanente de esta unidad con los puntos de coordinación previstos en el artículo siguiente, así como con los distintos responsables que en esta materia y de conformidad con lo previsto en el artículo 14, se establezcan en cada provincia."

La referencia del **artículo 9 apartado 4** al artículo 14 del proyecto de Orden, no parece coherente con el contenido del citado artículo, por lo que se sugiere su revisión.

10. Sobre los apartados 3 y 5 del artículo 12.

A. Artículo 12 apartado 3.

El **artículo 12** del proyecto de Orden, relativo a la Unidad de Seguridad TIC, regula en su **apartado 3**, las funciones de esta Unidad:

"3. Serán funciones de la Unidad de Seguridad TIC de la Consejería, conforme a lo dispuesto en el artículo 11.2 del Decreto 1/2011, de 11 de enero, las siguientes:

a) Prestar soporte, asesoramiento e información a los responsables de la estructura de seguridad de la Consejería y al Comité de Seguridad, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Diseñar y ejecutar los programas de actuación propios de la Consejería, incluyendo, entre otros, planes directores de seguridad, proyectos de desarrollo normativo, proyectos de seguridad operativa, auditorías técnicas y de cumplimiento y planes de adecuación legal.

c) Definir, Implantar y mantener los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización, supervisión y mantenimiento de los análisis de riesgos de la Consejería y la propuesta de las medidas necesarias para su tratamiento.

d) Revisar los análisis de riesgos de forma periódica, cuando existan cambios sustanciales en la información tratada o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves. A estos efectos, elaborará un listado de medidas organizativas y técnicas a implantar en el organismo, que elevará al Comité de Seguridad para su revisión y, en su caso, aprobación final.

e) Analizar los informes de auditorías, elevando al Comité de Seguridad las conclusiones.

f) Supervisar, de forma sistemática, los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas de la Consejería.

g) Definir y supervisar los criterios y requisitos técnicos de seguridad aplicados en las distintas fases del ciclo de vida de los soportes, sistemas y aplicaciones de la Consejería por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC, que incluye la definición de los requisitos y cláusulas de seguridad de los contratos de nuevos desarrollos, que deben estar actualizados en todo momento.

Adicionalmente, 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 a las personas responsables de la Información y responsables de los servicios correspondientes.

h) Elaborar y emitir un informe cuando, en el marco de una relación establecida con un tercero, éste no pueda satisfacer algún aspecto de la política de seguridad. El informe deberá precisar los riesgos en que se incurre y la forma de tratarlos, requiriendo la aceptación, en su caso, de las personas responsables de la información y responsables de los servicios afectados para continuar con la mencionada relación. Los referidos responsables deberán responder al informe en un plazo no superior a 30 días.

i) Definir y ejecutar los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito de la Consejería.

j) Coordinar, dirigir y realizar seguimiento de la actividad en materia de seguridad TIC de las entidades vinculadas o dependientes de la Consejería, desde el momento que se tenga conocimiento de la aprobación de la política de seguridad de dichas entidades.

k) Velar por la aplicación de los criterios y directrices de gestión de la seguridad TIC emanadas de la Unidad de Seguridad TIC de la Junta de Andalucía.

l) Gestión de la documentación de seguridad TIC.

m) Determinar la categoría del sistema, según el Esquema Nacional de Seguridad, tomando como base las valoraciones de impacto realizadas por los Responsables de la Información y los Servicios afectados en dicho sistema.

n) Cuantas otras le sean encomendadas"

En las **letras c) y d)** del **apartado 3** se propone incluir que las funciones detalladas en los mismos se desempeñarán con el asesoramiento del Delegado o Delegada 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 del citado Real Decreto.

B. Artículo 12 apartado 5.

El **artículo 12.5** del proyecto de Orden indica:

"5. La Unidad de Seguridad TIC realizará labores de apoyo a los Responsables del Tratamiento en la aplicación de medidas técnicas que sean competencia de dichos responsables. Entre dichas labores se incluirá la ejecución de análisis de riesgos de protección de datos de carácter personal, pudiendo intervenir el Delegado o Delegada de Protección de Datos para el asesoramiento y la supervisión en la materia."

En el **apartado 5** del **artículo 12** se aconseja la siguiente redacción para la **segunda frase**: *"Entre dichas labores se incluirá la ejecución de análisis de riesgos para los derechos y libertades de las personas físicas, interviniendo el Delegado o Delegada de Protección de Datos para el asesoramiento y la supervisión en la materia".* Con ello se persigue enfatizar la obligación establecida en el RGPD de gestionar el riesgo que, para los derechos y libertades de las personas físicas, supone un tratamiento, teniendo como principales manifestaciones el contenido de sus artículos 24, 32 y 35.

11. Sobre el artículo 16. Delegado o Delegada de Protección de Datos.

El **artículo 16** del proyecto de Orden dice:

"1. La Consejería y cada una de las entidades dependientes contará con una persona que ostente la condición de Delegado o Delegada de Protección de Datos, en los términos y con las atribuciones establecidos en la normativa vigente en materia de protección de datos de carácter personal.

2. La figura del Delegado o Delegada de Protección de Datos de la Consejería será nombrada por la persona titular de la Viceconsejería, entre el personal funcionario de la Consejería, atendiendo a los requisitos establecidos en el Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, y estará adscrito a ese órgano directivo. En el nombramiento deberá especificarse el alcance de su designación, que podrá alcanzar a una o varias de las entidades vinculadas o dependientes de la Consejería.

En dichas entidades el Delegado o Delegada de Protección de Datos será designada por la persona que asuma la máxima responsabilidad de la entidad correspondiente.

En todo caso, el Delegado o Delegada de Protección de Datos de la Consejería colaborará y se coordinará con las entidades vinculadas o dependientes de la misma en todas las cuestiones relativas a su ámbito de competencia, estableciendo mecanismos de colaboración con las personas responsables de protección de datos de dichas entidades.

3. El Delegado o Delegada de Protección de Datos podrá poner en conocimiento del Comité de Seguridad las cuestiones relacionadas con la protección de datos que considere necesarias.

4. Tendrá las funciones atribuidas en la normativa vigente en materia de protección de datos de carácter personal y, en particular, las siguientes:

a) Asesorar sobre la confección de los modelos de formularios de recogida de datos personales cuando el órgano directivo competente sobre el formulario lo considere conveniente, con el objetivo de supervisar que los mismos cumplen con lo establecido en los artículos 12 y 13 del Reglamento General de Protección de Datos.

b) Ser consultado sobre la contratación, análisis, diseño, operación y mantenimiento de todo tratamiento realizado sobre datos personales. También deberá ser consultado, con carácter preceptivo, sobre todo proyecto de norma dentro del alcance de su designación, que suponga un tratamiento de datos personales.

c) Asesorar sobre la evaluación de impacto relativa a la protección de datos de carácter personal, tanto en la necesidad de su realización como en su elaboración.

d) Supervisar, en los términos de lo dispuesto en el artículo 20, que el contenido del Registro de Actividades de Tratamiento se corresponda con las actividades efectivamente realizadas en la Consejería, debiendo los responsables facilitarle la información necesaria para ello.

e) Asesorar a los Responsables del Tratamiento sobre cómo proceder en relación con la notificación de incidentes de seguridad sobre datos personales a la autoridad de control correspondiente. También asesorará y dará apoyo a los Responsables del Tratamiento sobre la necesidad y manera de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales, conforme a lo establecido en el artículo 34 del Reglamento General de Protección de Datos.

f) Participar como vocal en las reuniones del Comité de Seguridad.

g) Supervisar la ejecución de las auditorías sobre protección de datos de carácter personal que se lleven a cabo en el ámbito de la Consejería."

Se sugiere incluir en el **primer párrafo** del **apartado 2** del **artículo 16**, en la **segunda frase,** una mención a los responsables de tratamiento, quedando redactada de la siguiente forma: *"En el nombramiento deberá especificarse el alcance de su designación, indicando los responsables de tratamiento para los que ejercerá sus funciones, que podrá alcanzar a una varias de las entidades vinculadas o dependientes de la Consejería".*

En el **último párrafo** del **apartado 2** se estima conveniente aclarar la condición o rol de "*las personas responsables de protección de datos*" de "*las entidades vinculadas o dependientes de la Consejería*" con las que el Delegado o Delegada de Protección de Datos de la Consejería establece mecanismos de colaboración

Se propone, asimismo, incluir un **nuevo párrafo final** del **apartado 2**, en el que se haga referencia a que la designación, nombramiento y cese del Delegado o Delegada de Protección de Datos de la Consejería sea notificada al Consejo de Transparencia y Protección de Datos de Andalucía, siguiéndose con ello lo establecido en el artículo 34.3 de la LOPDGDD en relación con el art. 37.7 del RGPD.

También se sugiere la inclusión en un **nuevo apartado** en el **artículo 16**, en el que se especifique el pleno respeto a la independencia del Delegado o Delegada de Protección de Datos de la Consejería en el ejercicio de sus funciones, de conformidad con lo dispuesto en los artículos 38.3 del RGPD y 36.2 de la LOPDGDD.

En relación al **apartado 4** del **artículo 16**, relativo a las funciones atribuidas al Delegado o Delegada de Protección de Datos, se aconseja añadir en la **letra c)**, sobre a la evaluación de impacto, la **expresión final** *"... así como supervisar su aplicación",* al estar dicha función expresamente contemplada en el artículo 39.1 c) del RGPD.

Asimismo, se propone aclarar el contenido de la **letra d)**, sustituyendo la palabra *"responsables"* por *"responsables del tratamiento".*

También se sugiere en la **letra e)** sustituir la palabra *"incidentes"* por *"violaciones"*, haciéndola coincidir con la que, como tal, figura en la frase siguiente de la citada **letra e)**; teniendo en cuenta, además, que el artículo 4.12) del RGPD incluye, entre sus definiciones, la de *"violación de la seguridad de los datos personales"*, que define como "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*". De igual forma, se entiende oportuno sustituir, en la **letra e)** la referencia genérica a la *"autoridad de control correspondiente"* por la expresa al "*Consejo de Transparencia y Protección de Datos de Andalucía",* como única autoridad de control competente en el ámbito en cuestión.

12. Sobre el artículo 17. Responsables del tratamiento.

El **artículo 17** del proyecto de Orden dispone:

"*1. La persona titular de cada órgano directivo tendrá la condición de Responsable del Tratamiento de datos personales en relación con aquellos que le sean accesibles por razón del ejercicio de sus competencias, y deberá determinar los fines y medios de su tratamiento. La condición de Responsable del Tratamiento coincidirá con la de Responsable de la Información.*

2. Los Responsables del Tratamiento tendrán las funciones y obligaciones establecidas en la normativa sobre protección de datos de carácter personal y, en particular, las siguientes:

a) Ser responsable del cumplimiento de lo dispuesto en el artículo 5.1 del Reglamento General de Protección de Datos y ser capaz de demostrarlo, para lo cual deberá aplicar las medidas técnicas y organizativas apropiadas.

b) Resolver las solicitudes de ejercicio de los derechos recogidos en los artículos 15 a 22 del Reglamento General de Protección de Datos, ambos inclusive. Asimismo, les corresponde informar al interesado sobre los derechos que le corresponden y sobre los medios disponibles para el ejercicio de estos derechos.

c) 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 los Servicios, de los Sistemas y, en caso de ser necesario, con el asesoramiento del Delegado o Delegada de Protección de Datos.

d) Verificar que los análisis de riesgos realizados se corresponden en todo momento con la información aportada para la realización de los mismos.

e) Garantizar la protección de datos de carácter personal desde el diseño y por defecto, en los términos establecidos en el artículo 25 del Reglamento General de Protección de Datos.

f) Poner en conocimiento del Delegado o Delegada de Protección de Datos la existencia de una violación de la seguridad de los datos personales. Asimismo, 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, se comunicará dicha circunstancia al interesado sin dilación.

g) Realizar la evaluación de impacto establecida en el artículo 35 del Reglamento General de Protección de Datos, cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas. El Responsable del Tratamiento recabará el asesoramiento del Delegado o Delegada de Protección de Datos para llevar a cabo esta evaluación de impacto.

h) Mantener un Registro de las Actividades de Tratamiento en los términos de lo establecido en el artículo 20. El Registro de Actividades de Tratamiento será público y accesible por medios electrónicos, y se encontrará continuamente actualizado.

i) Garantizar la concienciación y formación del personal que participa en las operaciones del tratamiento.

3. Los Responsables del Tratamiento deberán mantener un inventario de todos los Encargados del Tratamiento a los que han encargado la realización de actividades de tratamiento, con indicación de las actividades encomendadas. Dicho inventario, que deberá mantenerse actualizado, formará parte del registro de actividades de tratamiento y, cuando los Encargados del Tratamiento sean personas físicas, incorporará el dato del sexo de dichas personas, en cumplimiento del artículo 10.1.a) de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía."

En el **apartado 1** del **artículo 17** se aconseja la sustitución de la expresión "*La persona titular de cada órgano directivo* …" por la de "*Cada órgano directivo*…", habida cuenta que, tal y como se indica en las Directrices 07/2020 del Comité Europeo de Protección de Datos (CEPD) 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.

Además, teniendo en cuenta que, de conformidad con el artículo 4.7) del RGPD, el *"responsable del tratamiento"* se define como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento",* y por tanto, no tiene por qué acceder a los datos personales sobre los que determina los fines y los medios, en el mismo **apartado 1** se propone sustituir la frase "*...en relación con aquellos que le sean accesibles por razón del ejercicio de sus competencias*" por la frase"*...en relación con aquellos sobre los que determina los fines y los medios."*

Por iguales motivos, también se recomienda sustituir la redacción del **inciso final** del **apartado 1** (*"La condición de Responsable del Tratamiento coincidirá con la de Responsable de la Información*") por la de *"La condición de Responsable de la Información coincidirá con la de Responsable del Tratamiento".*

En la **letra c) del apartado 2** se aconseja sustituir la expresión "*...con la ayuda de los Servicios, de los Sistemas*..." por la de *"...con ayuda de los Responsables de los Servicios y de los Responsables de los Sistemas...".*

Para la **letra f) del apartado 2** se propone sustituir la actual redacción por la siguiente:

"f) Poner en conocimiento del Delegado o Delegada de Protección de Datos la existencia de una violación de la seguridad de los datos personales, efectuar la valoración del riesgo que la misma suponga para los derechos y libertades de las personas físicas y notificarla al Consejo de Transparencia y Protección de Datos de Andalucía sin dilación indebida, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para tales derechos y libertades. Asimismo, 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, la comunicará a los interesados sin dilación indebida".

Se considera que la misma resulta más acorde con el contenido de los artículos 33 y 34 del RGPD, además de concretar expresamente la autoridad de control competente en este ámbito.

En la **letra g) del apartado 2**, se considera conveniente incluir un añadido al **inicio de la primera frase,** que quedaría redactada así: *"Analizar los riesgos para los derechos y libertades de las personas físicas de los tratamientos de su responsabilidad y realizar la evaluación de impacto establecida en el artículo 35 del Reglamento General de Protección de Datos, cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para tales derechos y libertades"*.

En el **apartado 3** del **artículo 17**, en relación con los artículos 17.2 letra h) y 20 del proyecto de Orden (que establecen que "*El Registro de Actividades de Tratamiento será público y accesible por medios electrónicos*"), indicar que la obligación establecida a los responsables del tratamiento, en el artículo 31.2 de la LOPDGDD, de hacer público un inventario de sus actividades de tratamiento, en el que constará la información establecida en el artículo 30 del RGPD y su base legal, no alcanza la publicación de los encargados del tratamiento.

En cualquier caso, cuando se trate de encargados del tratamiento que sean personas físicas, la publicación de los mismos supondría un tratamiento de datos personales, por lo que se sugiere revisar la base legitimadora del mismo y el cumplimiento de los principios relativos al tratamiento del artículo 5 del RGPD. Además, en el supuesto de que se publiquen, los datos de los encargados del tratamiento que sean personas físicas deben ser los mínimos e imprescindibles para cumplir con la finalidad establecida, en consonancia con el citado artículo.

13. Sobre el apartado 2 del artículo 18.

El **artículo 18** del proyecto de Orden, relativo a los Encargados del Tratamiento, establece en su **apartado 2**:

"*Los Encargados del Tratamiento deberán cumplir todas las obligaciones que establezca la normativa vigente de protección de datos de carácter personal para esta figura y, especialmente, las que se establezcan en el contrato de encargo del tratamiento y proporcione el Responsable del Tratamiento directamente a la persona o entidad en la que recaiga el encargo.*"

Se propone una nueva redacción del **artículo 18.2**, con el fin de incidir en la obligación de que el encargado del tratamiento trate los datos personales siguiendo instrucciones documentadas del responsable del tratamiento, tal y como establece el artículo 28.3 letra a) del RGPD. La nueva redacción sería la siguiente:

"Los Encargados del Tratamiento deberán cumplir todas las obligaciones que establezca la normativa vigente de protección de datos personales para esta figura y las que se establezcan en el contrato o acto jurídico de encargo del tratamiento. En particular, tratarán los datos personales únicamente siguiendo las instrucciones documentadas del responsable del tratamiento".

14. Sobre el artículo 19. Incidencia de la normativa de protección de datos de carácter personal.

El **artículo 19** del proyecto de Orden señala:

"*1. Todos los tratamientos de datos personales que realice la Consejería se ajustarán a la normativa sobre protección de datos de carácter personal.*

En dicho ámbito, cada Responsable del Tratamiento de datos personales aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que los tratamientos de datos personales son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva. En caso de conflicto con otras normas de seguridad prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de datos de carácter personal.

2. Los Responsables y Encargados del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

3. En caso de violación de la seguridad de los datos personales, el Responsable del Tratamiento lo pondrá en conocimiento inmediato del Delegado o Delegada de Protección de Datos, que deberá asesorarle para proceder a notificar dicha violación a la autoridad de control competente sin dilación, de conformidad con lo dispuesto en el artículo 33 del Reglamento General de Protección de Datos.

Asimismo, 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 a la persona interesada sin dilación, de conformidad con el artículo 34 del Reglamento General de Protección de Datos.

4. Cuando sea probable que un tipo de tratamiento de datos personales, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona Responsable del Tratamiento realizará, antes del mismo, una evaluación del impacto de las operaciones de tratamiento en la protección de datos de carácter personal, de conformidad con el artículo 35 del Reglamento General de Protección de Datos. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos análogos, para ello, recabará el asesoramiento del Delegado o Delegada de Protección de Datos."

En consonancia con el ámbito de aplicación previsto en el artículo 1.2 letra b) del propio proyecto de Orden, se aconseja incluir en el **primer párrafo** del **apartado 1** del **artículo 19** una referencia a los tratamientos efectuados por las entidades vinculadas o dependientes de la Consejería, quedando así su redacción: *"Todos los tratamientos de datos personales que realice la Consejería y sus entidades vinculadas o dependientes se ajustarán a la normativa sobre protección de datos personales"*.

Se sugiere modificar la redacción del **apartado 2** al objeto de incidir, nuevamente, en la perspectiva de enfoque del riesgo en protección de datos, que resulta más amplia que en el ámbito de seguridad TIC. La redacción propuesta es la siguiente:

"Los Responsables y Encargados del Tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo que tales tratamientos pudieran entrañar para los derechos y libertades de las personas físicas".

El **apartado 3** presenta un contenido similar al del artículo 17.2 letra f) del proyecto de Orden, incorporando además las funciones del Delegado o Delegada de Protección de Datos recogidas en el artículo 16.4 e) del citado proyecto, por lo que se considera oportuna la modificación del art. 19.3 para ajustarlo a las propuestas efectuadas para los mencionados preceptos, quedando redactado en los siguientes términos:

"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 procederá a notificar dicha violación, con el debido asesoramiento del Delegado o Delegada de Protección de Datos, al Consejo de Transparencia y Protección de Datos de Andalucía sin dilación indebida, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para tales derechos y libertades.

Asimismo, 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, con el asesoramiento del Delegado o Delegada de Protección de Datos, la comunicará a los interesados sin dilación indebida".

En el **apartado 4**, de contenido similar al artículo 17.2 letra g) del proyecto de Orden, se sugiere una mínima modificación con vistas a mejorar su sintaxis, quedando su redacción de la siguiente forma:

"Cuando sea probable que un tipo de tratamiento de datos personales, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del Tratamiento realizará, antes del mismo, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, para lo que recabará el asesoramiento del Delegado o Delegada de Protección de Datos. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos análogos."

15. Sobre el apartado 2 del artículo 20.

El **artículo 20** del proyecto de Orden, relativo al Registro de Actividades de Tratamiento, dice en su **apartado 2**:

"*El Registro de Actividades de Tratamiento incluirá toda la información a la que se refiere el artículo 30 del Reglamento General de Protección de Datos, y será público y accesible por medios electrónicos, a través del apartado correspondiente a la protección de datos del portal web de la Consejería, y se encontrará continuamente actualizado*."

Sin perjuicio de lo indicado en el **artículo 20.2**, debe tenerse en cuenta que la publicación del Registro de actividades de tratamiento es una obligación de publicidad activa prevista en el artículo 6 bis de la LTAIBG así como que la información debe estar publicada en el Portal de la Junta de Andalucía, a la vista del artículo 18 de la LTPA. A su vez, los artículos 6 y 9.1 de la LTPA exigen que la información publicada lo sea de un modo que sea fácilmente comprensible y esté bien estructurada.

Por ello se recomienda, a los efectos de garantizar el cumplimiento de las normas citadas, que la información se publique en un único lugar del Portal de la Junta de Andalucía, evitando dobles publicaciones de una misma información, sin perjuicio de que en el apartado del Portal de la Junta de Andalucía correspondiente a la Consejería de Turismo, Cultura y Deporte se pueda incluir un enlace al Registro, ya publicado, con los resultados filtrados por la Consejería.

16. Sobre el apartado 1 del artículo 21.

El **artículo 21** del proyecto de Orden, que se ocupa de la gestión de riesgos, dispone en su **apartado 1**:

"*La gestión de riesgos debe realizarse de manera continua sobre los activos de la Consejería, así como sobre los tratamientos y los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica.*

En todo caso, para la evaluación y gestión de los riesgos se tendrán en cuenta los criterios que se establezcan con carácter general para la Junta de Andalucía y los específicos para la Consejería en los diferentes niveles de planificación, conforme a la normativa que resulte de aplicación."

En el **primer párrafo** del **apartado 1** se propone sustituir la expresión "tratamientos" por la de "tratamientos de datos personales", de manera que se especifique debidamente la naturaleza de los mismos.

17. Sobre el artículo 23. Gestión de incidentes de seguridad y de la continuidad.

El **artículo 23** del proyecto de Orden establece:

"*1. Ante incidentes de seguridad, el personal deberá actuar conforme a los mecanismos apropiados para su correcta prevención, detección, reacción y recuperación, habilitando un sistema de gestión que permita la mejora continua de la seguridad de los activos de la Consejería. En el caso de que dichas incidencias exijan una respuesta inmediata y coordinada, se convocará el Grupo de Respuesta a Incidentes de Seguridad contemplado en el artículo 8.5.*

2. En la gestión de los incidentes deberán integrarse aquellos procedimientos que establezca el órgano competente en materia de coordinación y ejecución de la política de seguridad interior y seguridad TIC de la Administración de la Junta de Andalucía o el Comité de Seguridad.

Igualmente, la Consejería actuará de forma coordinada con el Centro de Respuesta a Incidentes de Seguridad de la Junta de Andalucía.

3. Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas y mantener la continuidad de sus procesos, de acuerdo con las necesidades de nivel de servicio.

4. El Comité de Seguridad 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."

Se sugiere introducir en el **artículo 23** un **nuevo apartado** que contemple, específicamente, la notificación al Consejo de Transparencia y Protección de Datos de Andalucía, en el caso de que el incidente de seguridad constituya igualmente una violación de la seguridad de los datos personales.

18. Sobre el apartado 2 del artículo 26.

El **artículo 26** del proyecto de Orden, que trata de las relaciones con terceros, indica en su **apartado 2**:

"*Cuando la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de la política de seguridad regulada en la presente Orden y de la normativa de seguridad que aplique. Estos quedarán sujetos, a través de cláusulas contractuales o acuerdos de nivel de servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias.*

Se deberá garantizar que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad. Si la información es de carácter personal se estará a lo dispuesto en la normativa sobre protección de datos de carácter personal, especialmente respecto de aquellos terceros que se consideren Encargados del Tratamiento."

En el **apartado 2** del **artículo 26** 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 el **inciso final** del **segundo párrafo** del **apartado 2** se considera conveniente suprimir la mención a "*aquellos terceros que se consideren Encargados del Tratamiento*", para referirla únicamente a los Encargados del Tratamiento, puesto que, tal y como se define en el artículo 4.10) del RGPD, un "*tercero*" es una "*persona física o jurídica, autoridad pública, servicio u organismo distinto del … encargado del tratamiento*".

19. Sobre la disposición final segunda. Publicidad de la política de seguridad de la Consejería.

La **disposición final segunda** del proyecto de Orden señala:

"*A los efectos de su mejor difusión entre las personas empleadas de la organización y de otras partes interesadas, la presente Orden se publicará, además de en el Boletín Oficial de la Junta de Andalucía, en el portal corporativo y medios de difusión internos (Intranet) de la Consejería y sus entes instrumentales.*"

Se recomienda clarificar si cuando el precepto dice que "*se publicará …en el portal corporativo*" se está refiriendo al portal web de la Consejería (cuestión que parece ser la pretendida, conforme al tenor del precepto) o si, por el contrario, se refiere a la sección de transparencia del Portal de la Junta de Andalucía.

En este último caso, esto es, si la intención es que se publique en la sección de transparencia del Portal de la Junta de Andalucía, debería indicarse así expresamente, teniendo, además, en cuenta lo siguiente: tanto la Orden como la documentación del expediente correspondiente, deben publicarse en la sección de transparencia correspondiente, conforme a lo dispuesto en el artículo 13.1 de la LTPA, atendiendo a los momentos y trámites que se produzcan en el procedimiento (apartado de normativa en elaboración). Así mismo, una vez aprobada y publicada la norma, también deberá publicarse en la citada sección de transparencia, conforme a lo dispuesto en el artículo 13.2 de la LTPA (apartado normativa vigente).

Por tanto, y conforme a lo expuesto, si la finalidad del precepto es la de crear una obligación de publicidad activa distinta de las anteriores, debería modificarse la redacción indicando expresamente que deberá publicarse en la sección de transparencia del Portal de la Junta de Andalucía, así como el apartado en el que deberá publicarse, sin perjuicio de las obligaciones previstas en el artículo 13 de la LTPA, que serían independientes a esta publicación.

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

El presidente de la Comisión
Consta la firma
Jesús Jiménez López