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 ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONSEJERÍA DE AGRICULTURA, PESCA, AGUA Y DESARROLLO RURAL

I.- Con fecha 20 de marzo de 2024 ha tenido entrada en el Consejo de Transparencia y Protección de Datos de Andalucía solicitud de informe, efectuada por la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural, referente al proyecto de Orden por la que se establece la política de seguridad de la información de la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural.

Con la petición de informe se acompaña el proyecto de Orden, la Memoria justificativa, así como la Memoria justificativa del cumplimiento de los principios de buena regulación.

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 y 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. De carácter general sobre la regulación de la protección de datos personales.

Sin perjuicio de las observaciones de este informe referidas a artículos concretos, se estima oportuno realizar la siguiente observación de carácter general.

El proyecto de Orden aborda en diversos artículos la dimensión de la protección de datos personales (de manera explícita, al menos, en los artículos 9, 11, 17, 18, 19, 23 y 27 de la Orden), pero no realiza un tratamiento sistemático de la misma, quedando determinados aspectos, de especial relevancia, sin abordar. En particular, el "artículo 23. Seguridad de los Datos de Carácter Personal" resulta esencialmente declarativo.

Por ello, se recomienda la inclusión en la Orden de un capítulo completo dedicado a la protección de datos personales. En dicho capítulo se agruparían los diversos artículos ya presentes en el proyecto de Orden dedicados, exclusivamente, al ámbito de protección de datos (por ejemplo, el "artículo 17. Delegado/a de Protección de Datos", el " Artículo 18. Personas responsables y encargados de tratamientos de datos de carácter personal", entre otros) y se incluirían nuevos que contemplasen tanto las funciones y obligaciones de los principales actores involucrados en esta materia (delegado/a de protección de datos, responsables y encargados) como aspectos tales como la gestión los riesgos para los derechos y libertades de las personas físicas, la realización de evaluaciones de impacto relativas a la protección de datos, la gestión del registro de actividades de tratamiento, la gestión de violaciones de la seguridad de datos personales o la formación y concienciación al personal.

Alternativamente, la Consejería podría considerar abordar la elaboración de una política de protección de datos, de conformidad con el artículo 24.2 del RGPD.

2. 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) RGPD.

3. Sobre el “Artículo 1. Objeto”.

El artículo 1 del proyecto de Orden dispone:

“*1. La presente orden tiene por objeto establecer la política de seguridad de la información (en adelante PSI), en el ámbito de la Consejería de Agricultura, Pesca, Agua y Desarrollo Rural (en adelante Consejería), así como su marco organizativo y tecnológico. El alcance de la PSI engloba cualquier aspecto específico relativo a la política de seguridad de las tecnologías de la información y comunicaciones (en adelante TIC) y a la política de seguridad interior.*

2. La presente orden constituye el documento de política de seguridad de la información de la Consejería.”

La política de seguridad de la información no cita, dentro de su objeto, de forma explícita, el ámbito de la protección de datos personales. Se sugiere incorporar tal dimensión en el **art. 1**, dentro del objeto, ya que la misma se contempla, de manera explícita, en diversos artículos de la Orden.

4. Sobre el “Artículo 6. Principios básicos de la seguridad de la información”.

El artículo 6 del proyecto de Orden establece:

“*1. Los principios básicos que regirán la política de seguridad de la información de la Consejería serán los establecidos en el Esquema Nacional de Seguridad (en adelante ENS) por el artículo 5 del citado Real Decreto 311/2022, en la Política de Seguridad TIC de la Junta de Andalucía en el artículo 5 del Decreto 1/2011, de 11 de enero, y por la Política de seguridad interior en la Administración de la Junta de Andalucía, en el artículo 5 del Decreto 171/2020, de 13 de octubre, integrándose en los siguientes:*

a) Gestión integral de la seguridad: la seguridad se definirá y gestionará como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información de la Consejería, sobre los que se procurará el mantenimiento de sus dimensiones de confidencialidad, autenticidad, integridad, disponibilidad, trazabilidad y privacidad. Se prestará especial atención a la concienciación de los diferentes intervinientes en el proceso y sus superiores jerárquicos, con objeto de favorecer la necesaria coordinación imprescindible para minimizar los riesgos en la seguridad.

b) Gestión de la seguridad basada en riesgos: todos los sistemas incluidos en el alcance de esta política deberán estar incluidos en un análisis de riesgos que se realizará al menos anualmente, siguiendo una metodología reconocida, identificando y valorando los activos, evaluando las amenazas y las salvaguardas aplicadas. Se elaborará un informe del análisis de riesgos realizado y un plan de mejora de la seguridad de la

información para el tratamiento de dichos riesgos que revalúe la idoneidad de las medidas de seguridad existentes y las actualice cuando sea necesario, de acuerdo con el principio de proporcionalidad en costes económicos y operativos y con el principio de prioridad en la protección de las personas en relación a los activos.

Este análisis se revisará al menos cuando cambie la información manejada o los servicios prestados, cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades críticas.

c) Prevención, detección, respuesta y conservación. Se deben implementar las medidas de seguridad determinadas por las normas y leyes que le sean de aplicación, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles estarán claramente definidos y documentados, en orden a reducir la posible materialización de amenazas, favorecer su rápida detección y permitir una eficaz gestión de la respuesta y restauración de la información y servicios afectados.

Se adoptarán medidas que permitan detectar incidentes de seguridad y se establecerán canales adecuados para su comunicación y mecanismos para responder eficazmente a los incidentes en el menor tiempo posible, designando un punto de contacto para centralizar y gestionar el intercambio de información asociada a los incidentes de seguridad, así como estableciendo protocolos para el intercambio de información relacionada con dichos incidentes.

Se deberá garantizar en la medida de lo posible la disponibilidad de los servicios ofrecidos a la ciudadanía, en función de la criticidad de los mismos, así como la conservación de los datos e información en soporte electrónico.

d) Existencia de líneas de defensa. Se adoptará una estrategia de protección basada en múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, que permitan evitar en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad y desarrollar una adecuada reacción ante los mismos, evitando una afectación del conjunto de activos.

e) Principio de vigilancia continua y reevaluación periódica. Dado que los servicios se pueden degradar rápidamente debido a incidentes que, en función de su gravedad, pueden producir desde una simple desaceleración hasta la detención de los mismos, se debe monitorizar la operación de los servicios de manera continua para detectar anomalías en los niveles de prestación requeridos, actuando en consecuencia. La revisión de alertas, eventos y logs es especialmente relevante para establecer líneas de defensa. Para ello, se implantarán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente, a efectos de detectar cuándo se produce una desviación significativa de los parámetros de servicio marcados.

f) Principio de responsabilidad. Todas las personas que de una forma u otra participen en la utilización, operación, administración o gestión de un sistema de información, serán responsables de observar las normas de seguridad establecidas. Para ello las correspondientes responsabilidades deberán quedar determinadas de forma explícita, y ser comunicadas a cada una de ellas.

Se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema, estando diferenciada la responsabilidad sobre la explotación de los sistemas de información respecto a la responsabilidad de la seguridad.

g) Gestión de la seguridad en el ciclo de vida de los activos: los recursos informáticos y la información se encontrarán inventariados, con una persona responsable asociada y, en caso de ser necesario, una persona custodia de los mismos. Los inventarios se mantendrán actualizados para asegurar su validez. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería, en función de la cual se establecerán las medidas de seguridad exigidas para su protección, teniéndose en cuenta las especificaciones de seguridad en todas las fases del ciclo de vida de los mismos."

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 propone añadir el siguiente texto al **final** del **artículo 6 apartado 1, letra b)**:

"En los supuestos de sistemas de información que traten datos personales, contando con el asesoramiento del delegado de protección de datos, se realizará un análisis de riesgos conforme al artículo 24 del RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos."

5. Sobre el "Artículo 8. Estructura organizativa de la seguridad de la información".

El artículo 8 del proyecto de Orden dice:

"*1. La gestión de la 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, agrupadas en los siguientes bloques de responsabilidad:*

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

b) El desarrollo y/o explotación de sistemas de información.

c) La función de supervisión de la seguridad de los sistemas de información y de la seguridad interior.

2. La estructura organizativa básica de gestión de la seguridad de la información en el ámbito de la Consejería estará compuesta por los siguientes agentes:

a) Comité de Seguridad de la Información.

b) Unidad de Seguridad de la Información.

c) Unidad de Seguridad Interior y Puntos Coordinadores de Seguridad Interior.

d) Personas responsables de la Información.

e) Personas responsables de los Servicios.

f) Personas responsables de los Sistemas.

g) Persona responsable de Seguridad y Enlace de Infraestructuras Críticas.

h) Responsable de Seguridad de la Información de Servicios Esenciales.

i) Delegado/a de Protección de Datos.

j) Personas responsables o encargados de tratamientos de datos de carácter personal.

3. En cada una de las entidades vinculadas o dependientes existirá una estructura organizativa de gestión de la seguridad de la información que estará compuesta al menos por:

a) Comité de Seguridad Interior y de Seguridad TIC.

b) Personas responsables de la Información.

c) Personas responsables de los Servicios.

d) Personas responsables de los Sistemas.

e) Persona responsable de Seguridad.

f) Unidad de Seguridad Interior y Puntos Coordinadores de Seguridad Interior, si el Comité los considera necesarios por virtud del volumen o singularidad de los activos de la entidad.

g) Delegado/a de Protección de Datos.
h) Personas responsables o encargados de tratamientos de datos de carácter personal.

4 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, teniendo en cuenta las siguientes salvedades:

a) De acuerdo con el artículo 11.2 del Decreto 311/2022 y artículo 5.j) del Decreto 1/2011, de 11 de enero, la responsabilidad de la seguridad de los sistemas de tecnologías de la información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios, no pudiendo recaer en una misma persona la condición de responsable de seguridad y la de responsable de la información, servicios o sistemas.

b) Las que se deriven de la normativa reguladora en materia de Infraestructuras Críticas, Servicios Esenciales y Protección de Datos de Carácter Personal.

c) De conformidad con la organización interna de la Consejería, las responsabilidades que esta Orden asocie a las personas titulares de los centros directivos serán incompatibles con las de responsable de sistemas, de seguridad o de delegado/a de protección de datos.

5. Este modelo organizativo tiene el carácter de mínimo, pudiendo la Consejería o sus entidades vinculadas o dependientes crear subcomités o perfiles adicionales con responsabilidad en seguridad, para una mejor consecución de los objetivos y principios establecidos en esta Política mediante la ejecución de las funciones que se le puedan encomendar. Las propuestas de nuevas estructuras o perfiles de seguridad deberán ser remitidas, para su estudio y aprobación, al Comité de Seguridad de la Información, especificando la funciones que se le asignarán y, en caso de perfiles, las competencias requeridas para su desempeño.

6. Con sujeción al marco previsto por el ENS, por la normativa en materia de protección de datos, por la políticas de seguridad TIC y de seguridad interior de la Junta de Andalucía y por sus normativas de desarrollo, en las entidades vinculadas o dependientes de la Consejería la responsabilidad de la conformación y designación de estas figuras, recaerá sobre las propias entidades vinculadas o dependientes."

En los **apartados 2, letra j)** y **3, letra h) del art. 8**, conviene recordar que, tal y como se indica en las Directrices del Comité Europeo de Protección de Datos 07/2020 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 ello, se recomienda sustituir, en todo el texto del proyecto de Orden la expresión "Personas responsables o encargados de tratamientos de datos de carácter personal" o similares por "el responsable o encargado del tratamiento" al referirse a un órgano directivo.

En el **apartado 4, letra b) del art. 8** se propone incluir al final del párrafo la expresión "y en particular la posible existencia de conflicto de intereses", de conformidad con el artículo 38.6 RGPD.

6. Sobre el "9. Comité de Seguridad de la Información de la Consejería".

El artículo 9 del proyecto de Orden señala:

"*1. Se crea el Comité de Seguridad de la Información de la Consejería como órgano no colegiado de dirección y seguimiento en materia de seguridad de los activos físicos y de información de los que la Consejería sea titular o cuya gestión tenga encomendada. Estará adscrito al centro directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información.*

2. El Comité de Seguridad de la Información de la Consejería estará formado por los siguientes miembros:

a) La persona titular del centro directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información, que ejercerá la presidencia del Comité; la cual tendrá voto de calidad en la toma de decisiones del Comité en caso de empate.

b) La persona titular de la Coordinación del centro directivo de la Consejería que ostente las competencias en materia de Seguridad de la Información, que ejercerá la vicepresidencia del Comité.

c) La persona titular de cada uno de los Centros Directivos de la Consejería con rango de Viceconsejería o un representante, de nivel 28 o superior, por designación de la anterior, que actuará como vocal.

d) La persona titular del Centro Directivo de la Consejería al que corresponda la dirección del Organismo Pagador de Andalucía de Fondos Europeos Agrarios o un representante, de nivel 28 o superior, por designación de la anterior, que actuará como vocal.

e) La persona designada por la Agencia Digital de Andalucía, de nivel 28 o superior, como responsable del soporte que proporciona a la Consejería en materia de Tecnologías de la Información y Comunicaciones, que actuará como vocal.

f) Dos representantes, por designación de la persona titular de la Secretaría General Técnica, seleccionados entre las personas que ostenten las jefaturas de los Servicios de la Secretaría General Técnica con competencias en Legislación, Contratación, Personal y Administración General, que actuarán como vocales.

g) La persona que hubiere sido designada Delegado/a de Protección de Datos, que actuará como vocal.

h) La persona que hubiere sido designada Responsable de Seguridad y Enlace de las infraestructuras críticas responsabilidad de la Consejería, que actuará como vocal.

i) La persona que hubiere sido designada Responsable de Seguridad de la Información de los servicios de información de la Consejería categorizados como esenciales, que actuará como vocal. Si dicha designación hubiese recaído en un unidad u órgano colegiado, actuará como vocal la persona titular de la unidad o una persona designada por la presidencia del órgano colegiado.

j) La persona titular de la Unidad de Seguridad Interior, que actuará como vocal.

k) La persona titular de la Unidad de Seguridad de la Información, que actuará como vocal y que ejercerá la secretaría del Comité; podrá delegar esta función en un técnico/a de su Unidad, que asistiría a las reuniones del Comité con voz pero sin voto.

3. Se habilita el siguiente esquema de suplencias para el caso de que las personas titulares no puedan acudir a las reuniones del mismo.

a) Los vocales titulares de centros directivos podrán ser sustituidos por las personas titulares de las correspondientes Coordinaciones. Los vocales que ostenten la Coordinación de un centro directivo podrán ser sustituidos por la persona que designe de su propio centro de nivel 28 o superior.

b) Las personas titulares de centros directivos que designen vocales, deberán igualmente proponer sus posibles sustitutos.
c) Los restantes miembros podrán designar a una persona suplente que asuma sus funciones interinamente por ausencia o enfermedad; en caso de vacante, la designación se hará por la persona titular de la presidencia. Se procurará que la persona suplente pertenezca al mismo centro directivo que la persona vocal a la que suple y deberá contar además con similar cualificación y requisitos establecidos para el cargo.

4. En las designaciones de vocales y suplentes del Comité de Seguridad de la Información se procurará tener en cuenta la composición de género que permita la representación equilibrada de mujeres y hombres.

5. Serán funciones propias del Comité de Seguridad de la Información en el ámbito de la Consejería y sus entidades vinculadas o dependientes:

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

b) Aprobar las propuestas de creación de nuevas estructuras o perfiles de seguridad y ofrecer asesoramiento, de ser requerido, respecto al nombramiento de perfiles de seguridad.

c) Realizar tareas de coordinación con los Comités de Seguridad Interior y Seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería.

d) Velar por la coordinación entre los diferentes planes estratégicos en materia de seguridad de la información que puedan coexistir tanto en la Consejería como en sus entidades vinculadas o dependientes.

e) Informar regularmente a la persona titular de la Consejería del estado de la seguridad de la información en su ámbito.

f) Elevación de propuestas de revisión de la política de seguridad de la información de la Consejería, de directrices y normas de seguridad de la Consejería, o de revisión de los marcos normativos de seguridad interior y de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su reglamentaria tramitación.

6. Serán funciones propias del Comité de Seguridad de la Información en el ámbito de la Consejería:

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

b) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad de la información.

c) Promover la implantación y mejora continua del sistema de gestión de la seguridad de la información (en adelante SGSI) de la Consejería.

d) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos y priorizar las actuaciones en materia de seguridad en la Consejería.

e) Designar la Unidad de Seguridad de la Información de la Consejería entre las unidades existentes en la misma o ratificar la propuesta de cobertura de esta Unidad realizada por la Agencia Digital de Andalucía, de entre sus propias unidades y previa solicitud del Comité, garantizándose siempre el principio de función diferenciada.

f) Designar la Unidad de Seguridad Interior de la Consejería.
g) Designar a las personas responsables de los sistemas, o ratificar la propuesta de designación realizada por la Agencia Digital de Andalucía previa solicitud del Comité.

h) Dirimir cualquier posible conflicto respecto a la asignación de responsabilidades sobre la información y los servicios.

i) Establecer las normas básicas de funcionamiento del Grupo de Respuesta ante Incidentes de Seguridad de la Información y, en su caso, designar entre sus miembros a participantes en el mismo, adicionales a la composición mínima establecida en esta Política.

j) Identificación de la normativa aplicables a la Consejería en el ámbito de la Seguridad de la Información, manteniendo actualizado y aprobando el listado de requisitos legales aplicables.

k) Determinar los niveles de calificación de la información gestionada por la Consejería, estableciendo y documentando los criterios de aplicación.

l) Aprobación de los documentos del SGSI de la Consejería correspondientes al segundo y tercer nivel de los definidos en el artículo 22 de esta Política.

m) Coordinar los esfuerzos de todo el equipo humano con responsabilidad en materia de seguridad, elevando propuesta para la resolución de los conflictos de competencia que se puedan suscitar entre ellos, o resolviéndolos cuando el superior jerárquico de los mismos no pueda hacerlo o delegue su resolución.

n) Promoción de formación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la seguridad de la información entre el personal de la Consejería, aprobando los planes anuales de formación.

o) Coordinar y aprobar los planes de continuidad de la Consejería.

p) 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.

q) Supervisar el nivel de riesgo y la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos de información, monitorizando el desempeño de los procesos de gestión de incidentes de seguridad.

r) Impulsar la determinación de los niveles de seguridad de la información tratada, en la que se valorarán los impactos que tendrían los incidentes que afectaran a la seguridad de la información, todo ello con la participación de las personas Responsables de la Información correspondientes y de la Unidad de Seguridad de la Información.

s) Impulsar los preceptivos análisis de riesgos, junto a las personas Responsables de la Información y de los Servicios que correspondan, contando con la participación de la Unidad de Seguridad de la Información.

t) Establecer el nivel de riesgo aceptable, por encima del cual deberían adoptarse medidas enfocadas a la reducción del riesgo de las amenazas identificadas, y la aprobación de los planes de tratamiento que se definan a este respecto.

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

v) Coordinar las medidas técnicas y organizativas establecidas para el cumplimiento de 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 lapersona delegada de protección de datos."

En el **apartado 2, letra g) del art. 9**, se recomienda que la participación de la persona designada como Delegado/a de Protección de Datos en el Comité de Seguridad de la Información de la Consejería sea con voz, pero sin voto; a la vista de las funciones asesoras atribuidas a la misma por la normativa en materia de protección de datos, así como la obligación de que el desempeño de sus funciones no de lugar a conflicto de intereses,

Por otra parte, 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 sugiere redactar el **apartado 6, letra s) del art. 9** con el siguiente tenor:

"Impulsar los preceptivos análisis de riesgos, junto a las personas Responsables de la Información y de los Servicios que correspondan, contando con la participación de la Unidad de Seguridad de la Información. Cuando los sistemas de información traten datos personales, los análisis de riesgo también contemplarán los riesgos para los derechos y libertades de las personas físicas, de conformidad con el artículo 24 del RGPD, y se contará con la participación del Delegado/a de Protección de Datos.".

7. Sobre el "Artículo 10. Funcionamiento del Comité".

El artículo 10 del proyecto de Orden indica:

"*1. El Comité se reunirá con carácter ordinario al menos dos veces al año y, con carácter extraordiario cuando lo decida la persona titular de la presidencia, de oficio o a propuesta de alguno de sus miembros, y siempre que se produzcan incidencias de seguridad graves o surjan nuevas necesidades de seguridad que requieran la participación del Comité.*

2. El Comité 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, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, y los artículos 17 y 18 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. A los efectos de convocatorias, requisitos para celebración de sesiones, mayorías necesarias para adopción de acuerdos, votos dirimentes en caso de empate o funciones de sus integrantes, se estará a lo previsto en dichos artículos 17 y 18 de la Ley 40/2015, de 1 de octubre.

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

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

5. El Comité de Seguridad de la Información establecerá entre sus miembros un grupo de respuesta a incidentes de seguridad de la información y definirá sus normas básicas de funcionamiento, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los activos o sistemas de información críticos de la Consejería. Será el Presidente del Comité quien determine la existencia de tales contingencias. Las decisiones adoptadas por este grupo serán sometidas con prontitud al conocimiento del Comité y a la revisión posterior de su eficacia.

La composición mínima inicial de este grupo, que puede ser ampliada por el propio Comité, es la siguiente:

a) Persona titular de la presidencia del Comité de Seguridad de la Información.

b) Persona responsable de la Unidad de Seguridad de la Información de la Consejería.

c) Persona responsable de la Unidad de Seguridad Interior de la Consejería.

d) Persona o personas responsables de los Sistemas."

Al objeto de reforzar las garantías de la información transmitida durante las sesiones del Comité de Seguridad de la Información de la Consejería, se propone modificar la actual redacción del **apartado 2 del art. 10**, en la **parte central del inciso inicial** de la siguiente forma: "… 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".

Asimismo, con idéntico motivo, se propone añadir en el **apartado 2 del art. 10** un párrafo, 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 especializado que pueda ser convocado a las reuniones del Comité, se aconseja completar la redacción del **apartado 3 del art. 10**, añadiendo al final del mismo la siguiente frase:

"El personal técnico especializado convocado a las reuniones del Comité estará obligado a respetar la confidencialidad de toda la información a la que tengan acceso."

En el **apartado 5 del art. 10**, al objeto de poder analizar si un incidente de seguridad de la información también constituye una violación de seguridad de los datos personales contemplada en el artículo 35 RGPD, se sugiere incluir una nueva letra e) con el siguiente tenor: "Delegado/a de Protección de Datos, realizando funciones de asesoría."

8. Sobre el "Artículo 11. Unidad de seguridad de la Información".

El artículo 11 del proyecto de Orden dispone:

"*1. Es la unidad administrativa que asume la responsabilidad de que los servicios y sistemas de información se mantengan con el mayor grado de seguridad, atendiendo a los principios establecidos en esta Política y supervisando el SGSI implantado. Esta unidad tendrá las atribuciones en materia de seguridad TIC que establece el artículo 11.1 del Decreto 1/2011, de 11 de enero.*

2. La Unidad de Seguridad de la Información de la Consejería será nombrada o ratificada por el Comité de Seguridad de la Información, mediante acto documentado que se comunicará a la persona responsable que se encuentre a su frente. Esta designación deberá garantizar el cumplimiento del principio de función diferenciada recogido en el art. 11 del Esquema Nacional de Seguridad y en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

3. Sus funciones dentro del ámbito de la Consejería son:

a) Labores de soporte, asesoramiento e información al Comité de Seguridad de la Información, así como de ejecución de las decisiones y acuerdos adoptados por éste.

b) Supervisar el cumplimiento de la presente Política, y de sus normas y procedimientos derivados.

c) Asesorar en materia de seguridad de la información a los integrantes de la Consejería que así lo requieran.

d) Coordinación en materia de seguridad de la información en la Consejería y con otros organismos especializados.

e) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.

f) Categorizar los diferentes sistemas de información existentes en el ámbito de la Consejería y establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de seguridad definidos por las personas Responsables de los Servicios y de la Información afectados por el ENS, siguiendo en todo momento lo exigido en el Anexo II del ENS (Medidas de Seguridad).

g) Establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de protección de los datos de carácter personal, siguiendo en todo momento lo dispuesto en la normativa de Protección de Datos Personales.

h) Trasladar los requisitos y medidas de seguridad a aplicar durante el desarrollo de la actividad a las personas Responsables de sistemas, velando por su cumplimiento, para lo que deberá establecer directrices que posibiliten su demostración.

i) Desarrollo y seguimiento de programas de formación y concienciación en su ámbito de competencia.

j) Asesorar y participar en el proceso de la gestión de los riesgos a realizar por las personas Responsables de la Información, de los Servicios o de los Sistemas, en relación con la adquisición, incorporación desarrollo o modificación de productos o sistemas de información o en el desarrollo de nuevos proyectos.

k) Elevar un informe anual sobre el estado del proceso de gestión de riesgos al Comité de Seguridad de la Información.

l) Promover y realizar el seguimiento de las auditorías periódicas que den cumplimiento a las obligaciones en materia de seguridad de la información.

m) Analizar los informes de auditoría, presentando las conclusiones al Comité de Seguridad de la Información, transmitiendo con posterioridad los resultados a las diferentes personas responsables para que adopten las medidas correctoras oportunas.

n) Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, con inclusión y estudio de los incidentes más relevantes de cada período y la gestión realizada de los mismos, así como de los principales riesgos residuales asumidos por la organización, recomendando posibles actuaciones respecto de ellos.

4. Tendrá la condición de Responsable de Seguridad la persona responsable de la Unidad de Seguridad de la Información, o la designada desde ella para el ejercicio de estas funciones, y en virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que le corresponderán los deberes y responsabilidades correspondientes en los términos recogidos en el ENS y la guía CCN-STIC-801.

5. La Unidad de Seguridad de la Información de la Consejería elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de su categorización según el ENS y las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio y responsable del sistema. Dicho listado se entregará, actualizado, al Comité de Seguridad TIC del organismo

en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las mismas."

En la **letra e)** del **apartado 3 del art. 11**, para valorar si un incidente de seguridad afecta a datos personales, se sugiere incluir al final del mismo, la siguiente frase:

"Si el incidente de seguridad afectase a datos personales, se contactará con el responsable del tratamiento que actuará de acuerdo con lo establecido en el RGPD."

Tomando en consideración las funciones que el RGPD atribuye al delegado de protección de datos, y 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 se aconseja completar la redacción la **letra g)** del **apartado 3 del art. 11**, que quedaría como sigue:

"g) Establecer las medidas de seguridad adecuadas y eficaces para cumplir los requisitos de protección de los datos personales, siguiendo en todo momento lo dispuesto en la normativa de Protección de Datos Personales, para lo que deberá contar con el asesoramiento del delegado/a de protección de datos."

Finalmente, indicar que no se aprecia, entre las funciones explícitamente atribuidas a la Unidad de seguridad de la Información en el **art. 11**, la realización de los análisis de riesgos, aunque sí la de "*Asesorar y participar en el proceso de la gestión de los riesgos a realizar por las personas Responsables de la Información*" (art. 11, apartado 3 letra j). Por su parte, en el **artículo 13**, relativo a las Personas responsables de la información y de los servicios de la Consejería, **apartado 2 letra b)** se indica que los mismos proporcionarán "*la información necesaria a la Unidad de Seguridad de la Información para realizar los preceptivos análisis de riesgos*". Sin embargo, en el **apartado 3 del artículo 24** (Gestión de riesgos) sólo se contempla la función de revisión de los análisis de riesgos por parte de la Unidad.

En consecuencia, se aconseja revisar la redacción de los tres preceptos señalados para evitar la posible incertidumbre sobre en quien recae la obligación de realizar los análisis de riesgos.

9. Sobre el "Artículo 13. Personas responsables de la información y de los servicios de la Consejería".

El artículo 13 del proyecto de Orden establece:

"1. Los Responsables de la información y/o de los servicios serán las personas titulares de los centros directivos que decidan sobre la finalidad, contenido y uso de la información y/o sobre las características de los servicios a prestar, así como las que determinen los niveles de seguridad dentro del marco establecido en el anexo I del ENS.

2. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, los deberes y responsabilidades principales de estos perfiles 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 y/o de los servicios a prestar, identificando los niveles de seguridad de la información y/o servicios mediante la valoración del impacto sobre los mismos de los incidentes que pudieran producirse.

b) Determinar el nivel de calificación que debe aplicarse a la información bajo su responsabilidad y promover el correcto etiquetado de sus posibles soportes.

c) Proporcionar la información necesaria a la Unidad de Seguridad de la Información 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 (o las personas Responsables si hubiere varias).

d) En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

3. El nombramiento o renovación de estas figuras responsables se realiza en virtud de la presente política de seguridad de la información, estando aparejados automáticamente a la toma de posesión de la titularidad de los correspondientes centros directivos o unidades organizativas y a la adscripción a los mismos en cada momento de las distintas informaciones manejadas y servicios prestados."

En relación con el **apartado 1 del art. 13**, debe recordarse que el responsable de la información decidirá sobre la finalidad, contenido y uso de la información y que, en virtud del RGPD, tendrá la condición de responsable del tratamiento la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, así como que debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En consecuencia, en el apartado 1 del art. 13, se aconseja incluir el siguiente párrafo:

"Tendrá la consideración de responsable del tratamiento definido en el artículo 4.7 del RGPD el centro directivo cuya persona titular ostente la condición de responsable de la información, cuando la misma contenga datos personales, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan otra cosa."

10. Sobre el "Artículo 15. Persona responsable de Seguridad y Enlace de Infraestructuras Críticas".

El artículo 15 del proyecto de Orden dice:

"*1. La Consejería tiene la consideración de Operador de Infraestructuras Críticas, por lo que se encuentra obligada a la designación de una persona Responsable de Seguridad y Enlace con la Administración y a su comunicación formal a la autoridad competente, en base a lo dispuesto en el artículo 16.1 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.*

2. La persona Responsable de Seguridad y Enlace velará en el marco organizativo de la Consejería por la garantía de la seguridad de la información relativa a las infraestructuras críticas y a sus planes de protección, según la clasificación de la información almacenada.

3. Deberá ser informado y participar en el análisis y tratamiento de cualquier incidente de seguridad que afecte a la información y sistemas relativos a infraestructuras críticas, debiendo velar por su correcta resolución.

4. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

5. El Comité de Seguridad de la Información actuará como punto de coordinación respecto de otros posibles Operadores de Infraestructuras Críticas en el caso de que las mismas se localicen físicamente en instalaciones de la Consejería."

En el el **apartado 3 del art. 15**, para valorar si un incidente de seguridad afecta a datos personales, se sugiere incluir al final del mismo, la siguiente frase:

"Si el incidente de seguridad detectado afectase a datos personales, se contactará con el responsable del tratamiento que actuará de acuerdo con lo establecido en el RGPD."

11. Sobre el "Artículo 17. Delegado/a de Protección de Datos".

El artículo 17 del proyecto de Orden señala:

"1. La figura del Delegado/a de Protección de Datos, en los términos establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, en adelante RGPD), podrá ser asumida por una persona o grupo de personas de la Consejería, bien en base a la existencia de

una o más plazas específicas en la Relación de Puestos de Trabajo o bien por simple asignación de funciones, o por una persona externa, física o jurídica. En cualquiera de estos casos, se deberá acreditar a nivel personal conocimientos especializados en derecho y competencia en materia de protección de datos. Tendrá una adscripción dentro de la estructura de la organización a un órgano con competencias y funciones de carácter horizontal, a los efectos de poder relacionarse adecuadamente con la dirección de la organización y con las autoridades de control.

2. En los casos en que la figura esté atribuida a un grupo de personas de la Consejería, una de ellas ostentará la responsabilidad de su coordinación, convocará sus reuniones y ejercerá la función de su representación, quedando este hecho explícitamente recogido en el acto de nombramiento. Este grupo de trabajo podrá celebrar sus reuniones y adoptar acuerdos, 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, de conformidad con lo establecido en el artículo 91.3 de la Ley 9/2007, de 22 de octubre, y el artículo 17.1 de la Ley 40/2015, de 1 de octubre. Los acuerdos serán adoptados por mayoría de votos, teniendo la persona coordinadora del grupo voto dirimente en caso de empate.

3. El nombramiento o renovación de la figura del Delegado/a de Protección de Datos se realizará y comunicará, mediante acto documentado, por la persona titular de la Viceconsejería, con el parecer, si es requerido, del Comité de Seguridad de la Información de la Consejería.

4. El Delegado/a de Protección de Datos deberá desempeñar las funciones y responsabilidades asignadas a dicha figura por la normativa en materia de protección de datos recogida en el art. 23 de esta Orden.

5. El Delegado/a de Protección de Datos de la Consejería velará por la elaboración y mantenimiento de un registro unificado de tratamientos de datos de carácter personal, con indicación expresa de las personas u órganos que asumen las figuras de responsable del tratamiento, encargado del tratamiento y resto de requisitos exigidos por el art 30 del RGPD. Dicho listado se entregará actualizado al Comité de Seguridad de la Información de la Consejería en sus reuniones en caso de que haya sido modificado. Asimismo deberá informar de posibles deficiencias o faltas de información que se produzcan, de modo que el Comité pueda arbitrar los mecanismos necesarios para la subsanación de las mismas."

En el **apartado 2 del art. 17**, al objeto de reforzar las garantías de la información transmitida durante las sesiones telemáticas del grupo de DPDs, se propone modificar la actual redacción de la **parte final del segundo inciso**, de la siguiente forma: "… 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".

Asimismo, con idéntico motivo, se propone añadir al final del **apartado 2 del art. 17**, el siguiente inciso:

“Las personas miembros del grupo de DPDs están obligadas a respetar la confidencialidad de toda la información a la que tengan acceso”.

Se sugiere incluir en el **apartado 3 del art. 17**, una mención a los responsables de tratamiento, incluyendo, al final del mismo, el siguiente inciso:

“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”.

Además, en el **apartado 3 del art. 17** se propone incluir un nuevo párrafo en el que se haga referencia a que la designación, nombramiento y cese de la persona delegada de protección de datos de la Consejería sea notificada al Consejo de Transparencia y Protección de Datos de Andalucía, conforme a lo establecido en el artículo 34.3 LOPDGDD.

También se sugiere la inclusión de un **nuevo apartado**, a continuación del apartado 3 del art. 17, en el que se especifique el pleno respeto a la independencia de la persona delegada de protección de datos de la Consejería en el ejercicio de sus funciones, de conformidad con lo dispuesto en los artículos 38.3 RGPD y 36.2 LOPDGDD.

Finalmente, se propone completar el contenido del **apartado 5 del art. 17** para incluir la necesaria colaboración de los responsables del tratamiento en la elaboración del registro de actividades de tratamiento, así como mencionar, de forma expresa, la LOPDGDD a continuación de la mención al art .30 del RGPD, de forma que este apartado quedase redactado como sigue:

“5. El Delegado/a de Protección de Datos de la Consejería velará por la elaboración y mantenimiento de un registro unificado de tratamientos de datos personales, para lo que contarán con la colaboración de los responsables del tratamiento. En dicho registro constará indicación expresa de los órganos que asumen las figuras de responsable del tratamiento, encargado del tratamiento y resto de requisitos exigidos por el art 30 del RGPD y por el art. 31 de la LOPDGDD (o Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales). Dicho listado se entregará actualizado al Comité de Seguridad de la Información de la Consejería en sus reuniones en caso de que haya sido modificado. Asimismo deberá informar de posibles deficiencias o faltas de información que se produzcan, de modo que el Comité pueda arbitrar los mecanismos necesarios para la subsanación de las mismas.”

12. Sobre el “Artículo 18. Personas responsables y encargados de tratamientos de datos de carácter personal”.

El artículo 18 del proyecto de Orden dispone:

"*1. Los Responsables de los Tratamientos de datos de carácter personal de la Consejería serán los órganos directivos que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del RGPD.*

2. Los órganos directivos que realicen tratamientos de datos de carácter personal cuya responsabilidad resida en un tercero tendrán la consideración de encargado de tratamiento de conformidad con el artículo 4.8 del RGPD.

3. Los centros directivos, responsables o encargados de tratamientos, deberán desempeñar las funciones y responsabilidades asignadas a dichas figuras por la normativa en materia de protección de datos recogida en el art. 23 de esta Orden."

En relación a la observación realizada al artículo 8 del proyecto de Orden, se recomienda sustituir en todo el texto de la Orden la expresión "la persona responsable del tratamiento" por "el responsable del tratamiento" al referirse a un órgano directivo, al igual que para el concepto de "encargado".

En consonancia con el comentario realizado al artículo 13 del proyecto de Orden, se sugiere añadir al final del **apartado 1 del art. 18** la siguiente frase: "...y con apartado primero del artículo 13 de la presente Orden".

En este artículo resulta especialmente de aplicación la observación general realizada al inicio de este informe (ver su apartado IV. 1). En caso de que dicha observación no fuese atendida, se recomienda ampliar el **art. 18** recogiendo de forma más completa las funciones y obligaciones de los responsables del tratamiento, cuyo contenido debería contemplar el cumplimiento de los principios del tratamiento de datos personales recogidos en el artículo 5.1 RGPD, la gestión de las solicitudes de ejercicio de derechos de los artículos 15 a 22 RGPD, realizar o proporcionar la información necesaria para los análisis de riesgos en materia de protección de datos, la protección de datos desde el diseño y por defecto, la gestión de las violaciones de la seguridad de los datos personales, la realización de evaluaciones de impacto establecidas en el artículo 35 RGPD, la realización o supervisión del contenido del Registro de Actividades de tratamiento de su competencia, las acciones de concienciación y formación al personal y las obligaciones en la contratación de encargados del tratamiento, entre otras.

En el mismo sentido, debería ampliarse el contenido del **apartado 2 del art. 18** relativo al encargado del tratamiento, en el contexto del artículo 28 RGPD.

13. Sobre el "Artículo 19. Resolución de conflictos".

El artículo 19 del proyecto de Orden establece:

"1. En caso de conflicto entre diferentes personas, unidades u órganos responsables, éste será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad de la Información.

2. En los conflictos entre los responsables que componen la estructura organizativa de la política de seguridad de la información de la Consejería y los responsables definidos en virtud de la normativa de protección de datos de carácter personal prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal. En caso de conflicto en la determinación de dicho nivel de exigencia, prevalecerá la decisión del Comité de Seguridad de la Información.

3. En caso de conflicto de atribuciones se actuará de acuerdo a lo previsto en el artículo 110 de la Ley 9/2007, de 22 de octubre."

De conformidad con lo establecido en el artículo 36.4 LOPDGDD, se propone incluir el siguiente párrafo al final del **apartado 2 del art. 19**:

"En cualquier caso, cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a la persona titular del centro directivo que tenga la condición de responsable o el encargado del tratamiento."

14. Sobre el "Artículo 21. Terceras partes".

El artículo 21 del proyecto de Orden señala:

"*1. Cuando la Consejería preste servicios a otros organismos o maneje información de estos, se les hará partícipes de esta política de seguridad de la información, estableciéndose los canales que procedan para la comunicación y coordinación entre las respectivas organizaciones, en especial para una rápida y eficaz reacción ante incidentes de seguridad.*

2.Cuando la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel de servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo disponer la tercera parte de sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por 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 de la información.

3. Cuando algún aspecto de esta política de seguridad de la información no pueda ser satisfecho por una tercera parte según se requiere en el párrafo anterior, se requerirá un informe de la Unidad de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá que, antes

de continuar con las actuaciones, los responsables de la información y/o los servicios afectados asuman expresa y plenamente el informe."

En el **apartado 1 del art. 21**, en cumplimiento de lo establecido en el artículo 28 RGPD, se recomienda incluir una referencia a las violaciones de la seguridad de los datos personales como parte de los procedimientos de actuación. De esa forma se sugiere que el final del **apartado 1** se añada lo siguiente:

"…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 los dos últimos incisos del **apartado 2 del art. 21**:

"[…] 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 del art. 21** 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 esta les ceda o comunique información, según se infiere de lo dispuesto en el artículo 5.1 LOPDGDD.

15. Sobre el "Artículo 24. Gestión de riesgos".

El artículo 24 del proyecto de Orden indica:

"*1. La gestión de riesgos debe realizarse de manera continua sobre los activos de información e infraestructuras de la Consejería, conforme a los principios de gestión de la seguridad basada en los riesgos y de reevaluación periódica.*

2. El proceso de gestión de riesgos comprende las fases de identificación y valoración de la información manejada y de los servicios prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas.

3. Este análisis deberá revisarse por parte de la Unidad de Seguridad de la información, a partir de la información proporcionada y con la participación de los responsables de servicios, de la información y de los sistemas, al menos de forma anual o cuando se produzcan cambios importantes en la información manejada o los servicios prestados o ante vulnerabilidades e incidentes de seguridad graves. Como resultado, se elevará el correspondiente informe al Comité de Seguridad de la información, para el establecimiento del

nivel de riesgo aceptable y, cuando proceda, la propuesta de medidas a aplicar para evitar los riesgos identificados,así como de planes de tratamiento pertinentes.

4. Los responsables de la información y/o servicios son responsables de los riesgos sobre su información y/o servicios 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.

5. El Comité de Seguridad de la información realizará un seguimiento de los riesgos y de la eficacia de las medidas adoptadas para su tratamiento.

6. Para realizar el análisis de riesgos se utilizarán metodologías y herramientas reconocidas en el ámbito de la Administración Pública."

Se propone incluir un **nuevo apartado en el art. 24**, 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, realizará un análisis de riesgos teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento conforme al artículo 24 del RGPD. Los responsables del tratamiento, serán responsables de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo."

16. Sobre el "Artículo 25. Prevención, detección y respuesta frente a incidentes de seguridad y continuidad de los servicios."

El artículo 25 del proyecto de Orden dice:

"*1. La Consejería deberá estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en los artículos 8 y 25 del ENS.*

2. El Comité de Seguridad de la Información 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 mediant la combinación de controles de carácter organizativo, tecnológico y procedimental tanto preventivos como de recuperación.

3. A los efectos de una mejor gestión de los incidentes, se actuará de forma coordinada con el Centro de Respuesta a Incidentes de Seguridad de la Junta de Andalucía."

En el **apartado 3 del art. 25**, al objeto de poder gestionar adecuadamente las situaciones en las que un incidente de seguridad de la información constituye también una violación de seguridad de los datos personales contemplada en el artículo 35 RGPD, se sugiere incluir la siguiente frase al final de di-

cho apartado: "así como con el Delegado/a de Protección de Datos en los casos en que estén afectados datos personales."

17. Sobre el "Artículo 27. Auditorías y conformidad con la normativa".

El artículo 27 del proyecto de Orden dispone:

"*1. La Consejería realizará revisiones periódicas independientes sobre su SGSI, establecido para implementar esta Política de Seguridad, con objeto de garantizar el cumplimiento normativo vigente y su adecuación respecto a estándares internacionales de seguridad.*

2. Los sistemas de información de la Consejería serán objeto, al menos cada dos años, de una auditoría regular ordinaria interna y externa que verifique el cumplimiento de los requisitos del ENS. Independientemente, se realizarán aquellas auditorías que sean requeridas por otras normas o estándares que apliquen o se implanten en la Consejería. La Unidad de Seguridad de la Información realizará o, en su caso, coordinará, estas actividades de auditoría.

3. El sistema de seguridad interior de la Consejería serán objeto de una auditoría regular ordinaria interna o externa que verifique su funcionamiento respecto de las normas o estándares que apliquen o se implanten en la Consejería. La Unidad de Seguridad Interior realizará o, en su caso, coordinará, estas actividades de auditoría.

4. Con carácter extraordinario deberán realizarse dichas auditorías siempre que se realicen modificaciones sustanciales en el SGSI, en los sistemas de información y, en general, en los activos de la Consejería, que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas.

5. Los informes de auditoría quedarán a disposición del Comité de Seguridad de la Información. Por su parte, la Unidad de Seguridad de la Información y la Unidad de Seguridad Interior deberán analizar cada informe y elevar al Comité de Seguridad de la Información las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

6. La Consejería auditará su cumplimiento de la normativa de protección de datos de forma periódica, al menos cada dos años. La persona con funciones de Delegado de Protección de Datos realizará o, en su caso, coordinará, estas actividades de auditoría, trasladando el informe de auditoría y sus conclusiones a la Dirección de la Consejería."

En el **apartado 3 del art. 27**, al objeto de que se adopten las medidas correctivas necesarias identificadas en las citadas auditorías, se propone incluir la siguiente frase al final del citado apartado:

"...así como a los responsables del tratamiento, a fin de que adopten las medidas correctivas necesarias, y a la persona delegada de protección de datos."

18. 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.

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

El presidente de la Comisión

Consta la firma

Jesús Jiménez López