1. Disposiciones generales

CONSEJERÍA DE TURISMO, CULTURA Y DEPORTE

Orden de 15 de noviembre de 2023, por la que se establece la política de seguridad de la Consejería de Turismo, Cultura y Deporte en los ámbitos de seguridad interior, seguridad de las tecnologías de la información y comunicaciones y de la protección de datos personales.

La seguridad no es solo un valor jurídico, normativo o político, es igualmente un valor social. Es uno de los pilares primordiales de la sociedad, se encuentra en la base de la libertad y la igualdad y contribuye al desarrollo pleno de las personas.

En este sentido, a lo largo de las últimas décadas se ha ido configurando un complejo y amplio marco jurídico que atiende a la necesaria seguridad que debe producirse en los comportamientos de las Administraciones Públicas, en la gestión diaria de sus competencias, con la finalidad de salvaguardar la seguridad relativa a las personas y a los bienes que se ven afectados en el ejercicio de dicha gestión.

Es por ello que las Administraciones Públicas, en un ejercicio de responsabilidad y en base al marco jurídico aplicable, están desarrollando las políticas de seguridad que resultan necesarias en el ejercicio de su actividad y que atiendan a diferentes ámbitos materiales, tales como, la seguridad relativa a la protección de los datos personales, la seguridad de la aplicación de los medios electrónicos para el tratamiento de la información, la seguridad interior de los inmuebles, etc. Estas políticas, siendo de aplicación transversal y teniendo un mismo objetivo, confluyen en su aplicación práctica y, por tanto, requieren de una planificación y ejecución integral, siendo esta la vocación del presente texto normativo, con respecto a la política de seguridad de esta Consejería.

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 quien determine los fines y medios del tratamiento adopte medidas técnicas y organizativas para garantizar la seguridad adecuada al riesgo de los tratamientos de datos personales.

Entre los principios relativos al tratamiento de datos personales, el artículo 5.f) del Reglamento General de Protección de Datos determina que los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad».)

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 13.h) entre los derechos de las personas en sus relaciones con la Administraciones Públicas, hace referencia al derecho a la protección de los datos personales y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Asimismo, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en su artículo 3.2 establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculadas o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos personales y facilitarán preferentemente la prestación conjunta de servicios a las personas interesadas.

00293147

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, cuyo objeto es determinar la política de seguridad en la utilización de medios electrónicos, establece los principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 12 de dicho Real Decreto exige 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.

Para dar cumplimiento a los requisitos y finalidades del Esquema Nacional de Seguridad en su propio ámbito, la Junta de Andalucía aprobó el 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. En ellos se regula la organización de la seguridad de las tecnologías de la información y comunicación (en adelante TIC) en las distintas Consejerías y en sus entidades vinculadas o dependientes, así como la obligatoriedad de que las Consejerías dispongan de su propio documento de política de seguridad TIC, siendo el presente proyecto normativo el marco de la política de seguridad TIC para la Consejería de Turismo, Cultura y Deporte.

Por otro lado, 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 regula, en su Capítulo II un modelo organizativo funcional en el que por simplificación, eficacia y eficiencia se ha evitado la creación de un Comité de Seguridad, optando por incluir las que hubieran sido sus funciones y tareas entre las de los ya existentes comités de seguridad TIC.

A tal fin, el artículo 9 del Decreto 171/2020, de 13 de octubre, establece que «las respectivas normas de creación de los Comités a los que alude el artículo 10 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 de la Administración de la Junta de Andalucía, modificarán su denominación añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior y actualizando, de ser necesario, la composición y régimen de los mismos, con descripción incluso, de las nuevas funciones a incorporar».

Como consecuencia de lo expuesto, la presente Orden tiene la finalidad de establecer la política de seguridad de la Consejería de Turismo, Cultura y Deporte , englobando tres ámbitos materiales que requieren de una actividad proactiva y preventiva por parte de la Administración, tales como, la seguridad en el ámbito de las TIC, la seguridad interior y la seguridad relativa a la protección de datos personales.

En cumplimiento de la normativa vigente y, con el objetivo de crear el marco necesario y las condiciones imprescindibles para garantizar la seguridad y confianza en el ejercicio de las competencias que le son propias a esta Consejería, se establece la estructura de organización y gestión, y se desarrollan las directrices y principios básicos que deben regir las actuaciones en materia de seguridad TIC, seguridad interior y protección de datos personales, atendiendo a las especificidades que subyacen en la naturaleza de las atribuciones que son propias a la Consejería.

Finalmente, se ha incluido un artículo específico con el objetivo de posibilitar que otros ámbitos de la seguridad, como el que se refiere a la salvaguarda del patrimonio histórico, una vez sea implementado, se sume al esquema de seguridad regulado en la presente Orden, respondiendo así a la idea de seguridad integral que se persigue.

De conformidad con lo dispuesto en el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, en la elaboración de esta disposición se ha tenido presente la perspectiva de la igualdad de género.

También se ha tenido en cuenta la adecuación de la presente norma a los principios de buena regulación a los que se refiere el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En cumplimiento del principio de necesidad y eficacia, la presente Orden tiene una finalidad

00293147

clara, como es la de regular los aspectos, tanto organizativos como procedimentales, necesarios para la definición de la política de seguridad de la Consejería de Turismo, Cultura y Deporte a los efectos de cumplir con las obligaciones que le son propias en materia de seguridad, siendo el rango normativo proporcionado y coherente con la finalidad perseguida. Es proporcional y eficiente ya que evita la duplicidad de órganos y, de otro lado, no impone ningún tipo de medidas restrictivas de derechos u obligaciones.

En cuanto al principio de seguridad jurídica y a la justificación sobre el rango del proyecto normativo y su debida coherencia con el resto del ordenamiento jurídico, se resalta que la competencia para la aprobación de esta norma corresponde a la persona titular de la Consejería, al estar ante el ejercicio de la potestad reglamentaria prevista en el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y su forma, de conformidad con lo dispuesto en el artículo 46.4 del mismo cuerpo legal, debe ser la de orden.

Por otro lado, al tratarse de una norma organizativa que no afecta directamente a los derechos e intereses legítimos de la ciudadanía, se ha prescindido de los trámites de consulta, audiencia e información públicas, en virtud de lo dispuesto en los artículos 45.1.f) de la Ley 6/2006, de 24 de octubre; 133.4 (primer párrafo) de la Ley 39/2015, de 1 de octubre, y 28.2 de la Ley 7/2017, de 27 de diciembre, de Participación Ciudadana de Andalucía. Todo ello, sin perjuicio de los informes que, con carácter facultativo, se han recabado de aquellos órganos o entidades de la Administración autonómica cuyas competencias se entienden atañidas por el contenido de la Orden, así como de los correspondientes informes preceptivos.

En aplicación del principio de eficiencia, al estar ante una norma de carácter interno y organizativo, su aprobación no supondrá una carga administrativa, ni para las empresas ni para la ciudadanía.

La norma se compone de una parte expositiva, treinta artículos, una disposición adicional única, una disposición derogatoria única y tres disposiciones finales.

En su virtud, a propuesta de la Secretaría General Técnica, y en el ejercicio de las competencias que me confiere el artículo 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, y el artículo 26.2.a de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto y ámbito de aplicación.

1. En aplicación del artículo 12.2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la presente Orden tiene por objeto establecer la política de seguridad de la Consejería de Turismo, Cultura y Deporte (en adelante la Consejería) que engloba a los siguientes ámbitos:

a) Seguridad interior, en el marco de lo contemplado en el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior de la Junta de Andalucía y demás disposiciones que resulten de aplicación.

b) Seguridad de las tecnologías de la información y comunicaciones (en adelante TIC), en cumplimiento con lo establecido en el artículo 10.2 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, y demás disposiciones que resulten de aplicación.

00293147

c) Protección de datos personales, en el marco de lo recogido 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, así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás disposiciones que resulten de aplicación.

A efectos de la presente orden se entiende por política de seguridad de la Consejería a aquella que integra los tres ámbitos aludidos en el presente apartado.

2. Su ámbito de aplicación se extiende a:

a) La Consejería, tanto en sus servicios centrales como periféricos.

b) Las entidades vinculadas o dependientes de la Consejería, de conformidad con el artículo 10.3 del Decreto 1/2011, de 11 de enero, y sin perjuicio de que dichas entidades aprueben, en su caso, su propia política de seguridad en coherencia con la presente orden.

c) Toda persona que, aún no estando adscrita a la Consejería, tenga acceso a la información gestionada por la Consejería o a los sistemas de información de la misma.

Artículo 2. Definiciones, objetivos y principios.

Las definiciones, objetivos y principios básicos que regirán la política de seguridad de la Consejería serán los establecidos en:

a) 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).

b) La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales.

c) El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

d) El 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.

e) 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.

Artículo 3. Responsabilidad general.

1. La preservación de la seguridad, en los tres ámbitos que se regulan en la presente Orden, será considerada objetivo común de todas las personas al servicio de los órganos y entidades vinculadas o dependientes incluidos en el ámbito de aplicación de esta norma, siendo éstas responsables del uso correcto de la información a la que tengan acceso, de los activos que se vean involucrados en sus tareas durante el desempeño ordinario de sus funciones y actividades, así como de la detección precoz de cuantos indicios puedan servir a la prevención de riesgos para la seguridad de la información y la seguridad interior.

2. Todas las personas empleadas que presten servicios en la Consejería o en sus entidades vinculadas o dependientes tienen la obligación de conocer y cumplir la política de seguridad de la Consejería y las normas que le son de general aplicación, siendo responsabilidad del Comité de Seguridad Interior y de Seguridad TIC establecer mecanismos adecuados para que la información llegue a las personas afectadas.

3. Con carácter general, para el personal de la Consejería y de las entidades vinculadas o dependientes de la misma, regirán las normas de uso de los recursos TIC atendiendo al Código de Conducta en el Uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía, así como a cualesquiera otras instrucciones y normas que regulen el comportamiento

00293147

de las personas empleadas públicas en el uso de los sistemas informáticos y redes de comunicaciones de esta.

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.

5. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, obligación que será complementaria al deber de secreto profesional. Estas obligaciones se mantendrán aún cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

CAPÍTULO II

Organización de la política de seguridad

Artículo 4. Estructura organizativa.

1. La estructura organizativa de la política de seguridad de la Consejería se conforma mediante la siguiente estructura mínima:

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

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

1.º Unidad de Seguridad Interior.

2.º Puntos Coordinadores de Seguridad Interior.

3.º 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 previstos en el Decreto 171/2020, de 13 de octubre, teniendo en cuenta la definición del concepto de activo previsto en su Anexo I.

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

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

2.º Responsables de la Información.

3.º Responsables del Servicio.

4.º Responsables del Sistema.

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

1.º Delegado o Delegada de Protección de Datos.

2.º Responsables del Tratamiento.

3.º Encargados del Tratamiento.

2. En función de las necesidades y circunstancias de la organización, las funciones correspondientes a varios de estos perfiles podrán ser asumidas por una misma persona o grupo de personas, unidad administrativa o departamento. Las funciones del responsable del tratamiento también podrá recaer en un órgano administrativo, de los definidos en el artículo 5 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

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.

3. Este modelo organizativo, sin perjuicio de lo previsto en el artículo siguiente, tiene el carácter de mínimo. Las propuestas de nuevas estructuras o perfiles de seguridad deberán ser remitidas, para su estudio y aprobación, al Comité de Seguridad,

00293147

especificando las funciones que se le asignarán y, en caso de perfiles, las competencias requeridas para su desempeño, debiendo ser aprobada su creación por acuerdo del Comité de Seguridad.

Artículo 5. La seguridad de las entidades dependientes o vinculadas.

1. En las entidades dependientes o vinculadas a esta Consejería, las atribuciones que le son propias al Comité de Seguridad, serán asumidas por los consejos de dirección u órganos colegiados análogos que existan en las mismas.

2. Igualmente, en cada entidad dependiente o vinculada a esta Consejería deberá designarse a una persona Responsable de la Seguridad TIC así como un Responsable en materia de Seguridad Interior.

3. Los consejos de dirección u órganos colegiados análogos referidos en el apartado 1 se coordinarán con el Comité de Seguridad contemplado en el artículo 4.1.a), a través de las personas que asuman las responsabilidades de la seguridad TIC y de la Seguridad Interior.

Artículo 6. Naturaleza y composición del Comité de Seguridad Interior y Seguridad TIC.

1. La Consejería, atendiendo a lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero, contará con un Comité de Seguridad Interior y Seguridad TIC, como órgano colegiado interno cuyo funcionamiento y organización se regulará por lo establecido en esta Orden y por lo dispuesto en el Capítulo II del Título IV de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía y por Sección 3.ª, Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Comité de Seguridad desarrollará la dirección y seguimiento en materia de seguridad de la información y de los activos TIC y del tratamiento de datos personales de los que la Consejería sea titular a través del correspondiente responsable de la información, del servicio o del tratamiento, o cuya gestión tenga encomendada. Asimismo, y de acuerdo con lo dispuesto en el artículo 9 del Decreto 171/2020, de 13 de octubre, le corresponderá la dirección y el seguimiento en materia de seguridad interior.

Corresponde a la persona titular de la Secretaría General Técnica su impulso y organización, así como velar por su buen funcionamiento.

2. El Comité de Seguridad de la Consejería 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:

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

2.º La persona que ostente la representación legal de cada una de las entidades vinculadas o dependientes.

3.º 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, actuarán con voz y voto, conforme a lo dispuesto en el artículo 94.1.d) de la Ley 9/2007, de 22 de octubre, garantizando, en todo caso, que sus funciones y cometidos no den lugar a conflictos de intereses.

4.º Las personas titulares de las Coordinaciones Generales de la Viceconsejería y de la Secretaría General Técnica.

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

00293147

de dicho cargo, entre otras, las 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 acordada por el conjunto de miembros de dicho órgano colegiado, por un plazo máximo de cuatro años, prorrogable, una sola vez, por otros cuatro años.

3. En la composición, modificación o renovación del Comité de Seguridad se respetará la representación equilibrada de mujeres y hombres, conforme a lo establecido en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía y en el artículo 19.2 de la Ley 9/2007, de 22 de octubre.

4. En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la presidencia será sustituida por la persona titular de la vicepresidencia.

Tanto la vicepresidencia como las vocalías y la secretaría podrán designar a una persona suplente, con carácter permanente y aplicando un criterio de paridad entre mujeres y hombres, de entre personal funcionario a su servicio que ocupe puestos de trabajo de nivel 28 o superior, dando preferencia al personal funcionario con formación o experiencia en las materias sobre las que el Comité de Seguridad ejerce sus funciones. Dicha designación será comunicada a la Secretaría.

5. En todo lo no dispuesto por este artículo, el Comité de Seguridad se regirá por lo previsto en esta Orden, por la normativa reguladora de la política de seguridad en la Administración de la Junta de Andalucía, así como por el resto de la normativa aplicable, la reguladora del ENS y la de protección de datos de carácter personal.

Artículo 7. Funciones del Comité de Seguridad.

Serán funciones propias del Comité de Seguridad:

a) Aprobar el desarrollo de la normativa de seguridad TIC y 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 la Consejería de Empleo, Empresa y Comercio 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 artículo 11.1.e) del Decreto 1/2011, de 11 de enero.

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.

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

00293147

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 Delegaciones Territoriales de la Consejería asuman los Puntos Coordinadores de Seguridad.

h) Velar por la aplicación de la seguridad y protección de datos personales 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, 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 en los principios relativos al tratamiento de datos personales entre el personal de la Consejería y de las entidades instrumentales vinculadas o dependientes de la misma, 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 de los servicios de su competencia, obtenidos en el análisis de riesgos.

o) Monitorizar el desarrollo 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 normalizarla en el ámbito de aplicación de la presente Orden 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 a los Responsables 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.

s) Cuantas otras le sean encomendadas.

Artículo 8. Funcionamiento del Comité de Seguridad.

1. El Comité de Seguridad se reunirá de forma ordinaria, al menos, una vez por semestre. También podrá celebrar reuniones extraordinarias, si se produjeran incidentes

00293147

de seguridad graves o se produjeran conflictos que pudieran afectar gravemente a los servicios prestados por la Consejería.

Asimismo, se podrán celebrar reuniones extraordinarias en caso de modificaciones sustanciales del marco normativo de seguridad interior, seguridad TIC y protección de datos personales o de los riesgos a los que se encuentren expuestos los sistemas de información.

La evaluación de la oportunidad y conveniencia para convocar una reunión extraordinaria la realizará la persona titular de la vicepresidencia del Comité, que lo someterá a la presidencia del mismo. Todas las reuniones se realizarán previa convocatoria.

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, así como la integridad, confidencialidad y la autenticidad de la información entre ellas transmitida.

Las personas miembros del Comité de Seguridad están obligadas a respetar la confidencialidad de toda la información a la que tengan acceso.

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, estando obligados a respetar la confidencialidad de toda la información a la que tengan acceso, sin que en ningún caso pueda ocasionar coste económico.

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

5. El Comité de Seguridad establecerá entre sus miembros un Grupo de Respuesta a Incidentes de Seguridad que requieran una respuesta urgente y coordinada, y definirá sus normas básicas de funcionamiento. La función principal de este grupo 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 la presidencia del Grupo de Respuesta a Incidencias de Seguridad quien determine la existencia de tales contingencias. Las decisiones adoptadas por este grupo serán sometidas con prontitud al conocimiento del Comité Seguridad y a la revisión posterior de su eficacia.

La composición de este grupo será la siguiente:

a) La persona titular de la vicepresidencia del Comité de Seguridad.

b) La persona responsable de la Unidad de Seguridad TIC de la Consejería.

c) La persona responsable de la Unidad de Seguridad Interior de la Consejería.

d) La persona que ostente la condición de Delegado o Delegada de Protección de Datos.

e) Las personas Responsables de otras Unidades de Seguridad, en su caso.

Su composición podrá ser modificada mediante acuerdo del Comité de Seguridad.

6. El Comité de Seguridad aprobará por mayoría simple sus propias reglas de organización, funcionamiento y adopción de acuerdos.

7. En todo lo no previsto en este artículo, el Comité de Seguridad se regirá por esta Orden, por la normativa reguladora de la política de seguridad en la Administración de la Junta de Andalucía, así como por el resto de la normativa aplicable, la reguladora del ENS y de protección de datos de carácter personal.

Artículo 9. Unidad de Seguridad Interior.

1. La Consejería, de acuerdo con lo establecido en el artículo 10 del Decreto 171/2020, de 13 de octubre, contará con una Unidad de Seguridad Interior que desempeñará las atribuciones y funciones relacionadas en el citado artículo. La persona responsable de la unidad de Seguridad Interior y, en su caso, el resto de las personas componentes de la Unidad serán designados por el Comité de Seguridad a propuesta de la persona

00293147

titular del órgano directivo central de la Consejería de Turismo, Cultura y Deporte al que correspondan las competencias en materia de seguridad interior, entre personal funcionario que cuente con conocimientos específicos en esta materia.

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 y la propuesta de un Plan de Seguridad Interior para esta Consejería.

b) Proponer las adaptaciones necesarias al ámbito de la 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 esta Consejería 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 esta Consejería.

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

l) Asegurar en el ámbito de esta Consejería el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto, conforme a la normativa vigente en materia de protección de datos personales.

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

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

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

p) Proponer a la aprobación del Comité de Seguridad el Plan de Seguridad Interior de la Consejería de Turismo, Cultura y Deporte y de las entidades dependientes singulares.

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

3. La Unidad de Seguridad Interior, en el ejercicio de sus funciones, se coordinará con los órganos directivos centrales que tengan atribuidas competencias de gestión en relación con los diferentes activos a proteger.

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 la Unidad de Seguridad Interior 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 siguiente, se establezcan en las Delegaciones Territoriales de la Consejería.

00293147

Artículo 10. Puntos de Coordinación de Seguridad Interior.

1. A nivel provincial existirán Puntos Coordinadores de Seguridad Interior que serán asumidos por personal de las Delegaciones Territoriales de la Consejería designados al efecto por el Comité de Seguridad a propuesta de las personas titulares de dichos órganos periféricos.

2. Las atribuciones y funciones de los Puntos Coordinadores de Seguridad Interior serán las contempladas en el artículo 13 del Decreto 171/2020, de 13 de octubre, así como aquellas que se entiendan precisas y se recojan dentro de los diferentes niveles de planificación o resulten necesarias en su implementación, atendiendo a los criterios establecidos por el Comité de Seguridad o la Unidad de Seguridad Interior.

Artículo 11. Responsables de seguridad de activos singulares, conjuntos u otros bienes singulares o conjunto de ellos.

1. Dentro de la planificación que se apruebe por el Comité de Seguridad en materia de seguridad interior, de conformidad con lo contemplado en el artículo 4.3, se determinarán las personas que asuman roles específicos de responsabilidad en el ámbito de la seguridad interior con relación a los activos sobre los que ejerzan competencias de gestión directa, a propuesta de los órganos directivos centrales que resulten competentes por razón de la materia o por la entidad instrumental a la que se encuentre adscrita.

2. Las funciones que asumirán las personas responsables de seguridad deberán especificarse en los distintos niveles de planificación o podrán resultar de los criterios que, siendo precisos, sean fijados por el Comité de Seguridad o la Unidad de Seguridad Interior.

Artículo 12. Unidad de Seguridad TIC.

1. La Consejería contará con la Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

2. La persona titular de la Unidad de Seguridad TIC será designada, entre personal funcionario, por el Comité de Seguridad a propuesta de la persona titular del órgano directivo de la Agencia Digital de Andalucía que tenga atribuidas las competencias relacionadas con la estrategia y aplicación de las tecnologías de la información y de las comunicaciones.

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 ejecutar 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 la Consejería y lo elevará al Comité de Seguridad para su revisión y, en su caso, aprobación final.

Las funciones detalladas en las letras c) y d) de este apartado 3 se desempeñarán con el asesoramiento del Delegado o Delegada de Protección de Datos, de acuerdo con

00293147

lo previsto en el artículo 3.2 del Real Decreto 311/2022, de 3 de mayo, 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.

e) Analizar los informes de auditorías a los que se refiere el artículo 24 de esta orden, 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 en que se apruebe 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

4. La persona titular de la Unidad de Seguridad TIC tendrá la condición de Responsable de Seguridad TIC.

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 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.

6. La Unidad de Seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas, con indicación expresa de las personas u órganos que asumen las figuras de Responsable de la Información, Responsable del Tratamiento, Responsable del Servicio, Encargado del Tratamiento, Responsable del Sistema y Responsable de Seguridad TIC, para cada uno de ellas. Dicho inventario se entregará, actualizado, al Comité de Seguridad en cada una de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité de Seguridad disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

7. La Unidad de Seguridad TIC podrá ejercer como Responsable de Seguridad TIC de las entidades vinculadas o dependientes de la Consejería si es nombrada como tal por

00293147

el Comité de Seguridad, previo informe favorable del órgano directivo del que dependa jerárquicamente dicha Unidad.

8. La Unidad de Seguridad TIC mantendrá un registro actualizado de las normas aplicables a la Consejería en materia de seguridad TIC y de protección de datos personales. Para ello, la Unidad de Seguridad TIC actuará de forma coordinada con el Delegado o Delegada de Protección de Datos.

Artículo 13. Responsables de la Información.

1. La persona titular de cada órgano directivo tendrá la condición de Responsable de la Información, según el Esquema Nacional de Seguridad, de toda información sobre la que tenga capacidad para decidir sobre su finalidad, contenido y uso. La condición de Responsable de la Información coincidirá con la de Responsable del Tratamiento.

2. Los Responsables de la Información tendrán las funciones que establece para ellas el Esquema Nacional de Seguridad y, en particular, las siguientes:

a) Determinar los requisitos de la información, mediante la valoración de la información derivada de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de Responsables de los Servicios y Responsables de los Sistemas afectados.

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

Artículo 14. Responsables del Servicio.

1. La persona titular de cada órgano directivo o una unidad administrativa con rango de servicio, integrada en dicho órgano directivo y designada por la persona titular del mismo, tendrá la condición de Responsable del Servicio, según el Esquema Nacional de Seguridad, para aquellos servicios sobre los que se decida por sus características y requisitos.

2. Los Responsables de los Servicios tendrán las funciones que establece para ellos el Esquema Nacional de Seguridad y, en particular, las siguientes:

a) Determinar los requisitos de los servicios a prestar mediante la valoración de los impactos de los incidentes que puedan producirse.

b) Proporcionar la información necesaria a la Unidad de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar. Para ello contará con la ayuda de Responsables de la Información y Responsables de los Sistemas afectados.

c) Aceptar los riesgos residuales de los servicios prestados que se identifiquen en el análisis de riesgos y realizar su seguimiento y control, sin prejuicio de la posibilidad de delegar esta tarea.

d) Asegurarse de que los permisos necesarios para el acceso a los diferentes aplicativos informáticos correspondientes al personal que ya no tenga que acceder al servicio prestado, se revoquen o deshabiliten en los sistemas relacionados.

Artículo 15. Responsables del Sistema.

1. Tendrán la condición de Responsables del Sistema la persona o personas encargadas de implantar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Los Responsables de los Sistemas tendrán las funciones que establece para ellas el Esquema Nacional de Seguridad y, en particular, las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo la definición de especificaciones, instalación y verificación de su correcto funcionamiento.

00293147

b) Velar por que la seguridad de la información esté presente en todas y cada una de las partes del ciclo de vida de los sistemas de información de los que es responsable. Especialmente deberá velar por que el desarrollo de los sistemas de información siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía. Para todo ello, podrá contar con el asesoramiento de la Unidad de Seguridad TIC.

c) Crear, mantener y actualizar de manera continua la documentación de seguridad de los sistemas de información, con el asesoramiento de la Unidad de Seguridad TIC.

d) Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

e) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

f) Acordar, en caso necesario, la suspensión del manejo de determinada información o de la prestación de un determinado servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser consensuada con los Responsables de la Información y los Servicios afectados y con el Responsable de Seguridad TIC, antes de ser adoptada. En caso de desacuerdo se aplicará lo establecido en el artículo 25.

g) 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 Responsables de la Información y de los Servicios afectados.

3. La persona Responsable del Sistema será designada por el Comité de Seguridad, garantizando el principio de función diferenciada previsto en el artículo 5.j) del Decreto 1/2011, de 11 de enero, que exige que la responsabilidad de la seguridad de los sistemas de información y comunicaciones estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Artículo 16. Delegado o Delegada de Protección de Datos.

1. La Consejería y cada una de sus entidades vinculadas o 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 personales.

2. El Delegado o la 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, indicando los responsables de tratamiento para los que ejercerá sus funciones, que podrá alcanzar a una o varias de las entidades vinculadas o dependientes de la Consejería.

En las entidades vinculadas o dependientes de la Consejería, el Delegado o Delegada de Protección de Datos será designada por la persona que asuma la dirección 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.

La designación, nombramiento y cese del Delegado o Delegada de Protección de Datos de la Consejería será notificada al Consejo de Transparencia y Protección de Datos de Andalucía, siguiéndose con ello lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y a la Ley Orgánica 3/2018, de 5 de diciembre.

3. De conformidad con lo dispuesto en en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y a la Ley Orgánica 3/2018, de

00293147

5 de diciembre, el Delegado o la Delegada de Protección de Datos de la Consejería, en el ejercicio de sus funciones, actuará con plena independencia.

4. 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.

5. Tendrá las funciones atribuidas en la normativa vigente en materia de protección de datos personales 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, en todo proyecto de norma que incluya en su contenido el tratamiento de datos personales.

c) Asesorar sobre la evaluación de impacto relativa a la protección de datos personales, tanto en la necesidad de su realización como en su elaboración, así como supervisar su aplicación.

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 del tratamiento facilitarle la información necesaria para ello.

e) Asesorar a los Responsables del Tratamiento sobre cómo proceder en relación con la notificación de violaciones de seguridad sobre datos personales al Consejo de Transparencia y Protección de Datos de Andalucía. 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 personales que se lleven a cabo en el ámbito de la Consejería.

Artículo 17. Responsables del Tratamiento.

1. Cada órgano directivo tendrá la condición de Responsable del Tratamiento de datos personales en relación con aquellos sobre los que determina los medios y los fines del tratamiento. La condición de Responsable de la Información coincidirá con la de Responsable del Tratamiento.

2. Los Responsables del Tratamiento tendrán las funciones y obligaciones establecidas en la normativa sobre protección de datos personales 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 Responsables de los Servicios y de los Responsables de los Sistemas y, en caso de ser necesario, con el asesoramiento del Delegado o Delegada de Protección de Datos.

00293147

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 personales 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, 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, procederá a comunicar a las personas físicas interesadas el probable alto riesgo que pueda entrañar la violación de la seguridad de sus datos personales en sus derechos y libertades.

g) 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 el tratamiento entrañe un alto riesgo para tales derechos y libertades. 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.

Artículo 18. Encargados del Tratamiento.

1. Los Responsables del Tratamiento podrán encargar a otros órganos, así como a otras personas físicas o jurídicas, la ejecución de actividades de tratamiento de datos personales siempre que acrediten, con carácter previo a su contratación, que ofrecen garantías suficientes para aplicar medidas técnicas y organizativas acordes al tratamiento que se les encomiende.

2. 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".

CAPÍTULO III

Desarrollo de la política de seguridad

Artículo 19. Incidencia de la normativa de protección de datos personales.

1. 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. 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

00293147

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 personales.

2. 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.

3. 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.

Artículo 20. Registro de Actividades de Tratamiento.

1. La Consejería contará con un Registro de Actividades de Tratamiento en el que cada Responsable del Tratamiento inscribirá su actividad bajo su responsabilidad, siendo la administración, coordinación y control de este registro una de las funciones a desarrollar por el Delegado o Delegada de Protección de Datos de la Consejería.

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.

Artículo 21. Gestión de riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre los activos de la Consejería, conforme a lo dispuesto en el Decreto 171/2020, de 13 de octubre, así como sobre los tratamientos de datos personales 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.

2. El proceso de gestión de riesgos comprenderá las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar debidamente justificadas. Dicho proceso deberá revisarse cada año por parte de los responsables de las Unidades de Seguridad de la Consejería, que elevarán un informe al Comité de Seguridad. En la medida en la que los riesgos afecten a los tratamientos de datos personales, el Delegado o Delegada de Protección de Datos participará en esta revisión.

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

4. Para realizar el análisis de riesgos se utilizarán metodologías y herramientas reconocidas en la normativa que resulta de aplicación para el ámbito de la Administración Pública.

5. Los Responsables de la Información y de los Servicios son responsables de establecer los requisitos de la información y los servicios en materia de seguridad 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.

Artículo 22. Clasificación de activos.

Los activos de la Consejería, conforme a lo dispuesto en el Decreto 171/2020, de 13 de octubre, estarán clasificados de acuerdo con su sensibilidad y criticidad para el

00293147

desarrollo de la actividad de la misma, en función de la cual se establecerán las medidas de seguridad exigidas para su protección, todo ello atendiendo a los criterios que se recojan en los distintos planes de seguridad que se elaboren y resulten de aplicación.

Artículo 23. Gestión de incidentes de seguridad y de la continuidad.

1. Ante incidentes de seguridad, el personal deberá actuar conforme a los mecanismos apropiados para su correcta prevención, detección, reacción y recuperación, para ello, las unidades competentes habilitarán un sistema de gestión que permita la mejora continua de la política de seguridad. 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 desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones y de política de seguridad interior de la Administración de la Junta de Andalucía y del sector público andaluz.

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.

5. En caso de que el incidente de seguridad constituya una violación de la seguridad de los datos personales, se notificará al Consejo de Transparencia y Protección de Datos de Andalucía.

Artículo 24. Auditorías de seguridad.

1. Al menos cada dos años, o con carácter específico y extraordinario cuando se lleven a cabo modificaciones sustanciales que repercutan en el cumplimiento de las medidas implantadas, o ante la existencia de elementos que puedan evidenciar la posible manifestación de un riesgo no evaluado o no previsto, o cuando se estime necesario por el Comité de Seguridad, se realizarán auditorías de seguridad a fin de verificar el cumplimiento de los requerimientos de la presente política, del ENS, o de cualquier otra norma que así lo requiera.

Estas auditorías se llevarán a cabo de conformidad con lo establecido en las normas de los diferentes ámbitos de seguridad aludidos en la presente orden.

El alcance de las auditorías deberá incluir la adopción de las medidas técnicas y organizativas que se apliquen para garantizar la seguridad que se requiera para cada caso.

En relación con los sistemas de información de categoría básica, esta auditoría podrá ser sustituida por una autoevaluación en los términos establecidos en el Esquema Nacional de Seguridad.

2. La Unidad de Seguridad Interior, la Unidad de Seguridad TIC y, en el caso en que le afecte, el Delegado o Delegada de Protección de Datos, supervisarán las auditorías y emitirán las recomendaciones que estimen oportunas en sus respectivos ámbitos de actuación.

Los informes de auditoría, bajo el conocimiento y supervisión del Comité de Seguridad, serán presentados ante los responsables de las unidades aludidas en el párrafo anterior, así como ante el Delegado o Delegada de Protección de Datos, para la valoración de las medidas correctoras propuestas en sus respectivos ámbitos de competencias. Estos, en el plazo que se estime conveniente por el Comité de Seguridad, presentarán sus conclusiones y propuestas para que el Comité de Seguridad apruebe las medidas

00293147

correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y normas de seguridad.

3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre los diferentes ámbitos de seguridad, siempre que sea posible, las auditorías que se encarguen deberán analizar de forma conjunta los diferentes ámbitos de la seguridad que son objeto de la presente orden.

Artículo 25. Resolución de conflictos.

1. Los conflictos entre las diferentes personas, unidades u órganos responsables que componen la estructura organizativa de la política de seguridad serán resueltos por el Comité de Seguridad.

2. En los conflictos entre las personas responsables que componen la estructura organizativa de la seguridad TIC y las personas responsables definidas en la normativa de protección de datos personales, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 26. Relaciones con terceros.

1. Cuando la Consejería preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de la política de seguridad definida en la presente orden, estableciendo los canales y mecanismos que procedan para la comunicación y coordinación entre las respectivas organizaciones y los procedimientos de actuación frente a los incidentes de seguridad que procedan.

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 la política de seguridad regulada en la presente orden.

Los terceros cuyos servicios sean utilizados por la Consejería o a los que ésta les ceda o comunique información estarán sometidos al deber de confidencialidad y no difusión de los datos que se intercambien o a los que pueda tener acceso en el contexto de su relación profesional o comercial.

Si la información es de carácter personal se estará a lo dispuesto en la normativa sobre protección de datos personales respecto de los Encargados del Tratamiento.

3. Cuando algún aspecto de la política de seguridad TIC regulada en la presente orden no pueda ser satisfecho por el tercero, la Unidad de Seguridad TIC realizará un informe que precise los riesgos en que se incurre y la forma de tratarlos, el cual deberá ser aprobado por los responsables de la información y de los servicios afectados antes de proseguir en la relación con el tercero, adoptando las medidas necesarias en función de en qué concluya el informe.

4. La Consejería podrá contar con la ayuda de terceros para mejorar los sistemas de seguridad que se implementen como consecuencia de la política de seguridad, mediante la contratación de auditorías, asistencias técnicas o desarrollos especializados.

Artículo 27. Formación y divulgación.

1. El Comité de Seguridad aprobará un Plan Anual de Formación sobre la política de seguridad, dentro del cual se contemplará, para cada año, el desarrollo de actividades de formación, divulgación y concienciación sobre tratamiento de datos personales, seguridad interior y seguridad TIC destinadas a las personas empleadas públicas incluidas en el ámbito de aplicación de la presente orden.

00293147

2. En la realización de esta actividad se tendrá en cuenta el Plan de Formación del Instituto Andaluz de Administración Pública para complementarlo con las acciones de la propia Consejería que sean necesarias.

3. El Delegado o Delegada de Protección de Datos supervisará las acciones de formación y divulgación del personal que participa en las operaciones de tratamiento con datos personales.

Artículo 28. Desarrollo, revisión y difusión de la política de seguridad.

1. La política de seguridad deberá mantenerse actualizada a las circunstancias técnicas u organizativas y evitar su obsolescencia.

2. La normativa reguladora de la seguridad interior, de la seguridad TIC y de la protección de datos de la Consejería, y su posterior desarrollo, será de obligado cumplimiento.

3. Las revisiones y actualizaciones de la política de seguridad que se regulan en la presente orden se propondrán por el Comité de Seguridad y se aprobarán por la persona titular de la Consejería.

4. A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la política de seguridad se publicará y divulgará, además de en el Boletín Oficial de la Junta de Andalucía, a través de los medios que se establezcan por el Comité de Seguridad.

Artículo 29. Integración de Planes.

Conforme a lo contemplado en el artículo 17.4 del Decreto 171/2020, de 13 de octubre, el Plan de Seguridad Interior de la Consejería establecerá los planes autónomos o integrados o de contenido compartido con otros planes, relacionados o no con la seguridad, cuya elaboración y aprobación resulte de carácter obligatorio para la Consejería por así venir contemplado en leyes o normas de carácter sectorial, tales como la relativa a la salvaguarda del Patrimonio Histórico.

Artículo 30. Cooperación en materia de seguridad TIC.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la seguridad de la información, se fomentará, en coordinación con la Unidad de Seguridad TIC Corporativa para los agentes externos a la Junta de Andalucía, el establecimiento de mecanismos de coordinación con al menos los siguientes agentes:

a) La Agencia Digital de Andalucía.

b) El Comité de Seguridad Interior y Seguridad TIC de la Junta de Andalucía.

c) La Unidad de Seguridad TIC de la Junta de Andalucía.

d) AndalucíaCERT (centro especializado y orientado a la prevención, detección y respuesta a incidentes y amenazas de seguridad).

e) El Consejo de Transparencia y Protección de Datos de Andalucía.

f) CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.

g) La Agencia Española de Protección de Datos (AEPD).

h) El Instituto Nacional de Ciberseguridad (INCIBE).

i) El Departamento contra el cibercrimen de la Guardia Civil y Brigada Central de Investigación Tecnológica del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

Adicionalmente, se podrán mantener contactos con otros organismos y entidades, incluyendo los entes instrumentales de la Consejería.

00293147

Disposición adicional única. Constitución del Comité de Seguridad.

1. La primera convocatoria del Comité de Seguridad tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de tres meses a partir de la entrada en vigor de la presente orden. Durante la celebración de la sesión constitutiva se procederá a realizar las designaciones que competen a este órgano según lo dispuesto en la presente orden.

2. Asimismo, en la sesión constitutiva del Comité de Seguridad y para aquella información, servicios y sistemas que se encuentren inventariados, se verificarán las designaciones de los Responsables de la Información, del Servicio y del Sistema.

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden.

Disposición final primera. Habilitación para la ejecución.

Se faculta a la persona titular de la Viceconsejería para dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas para la difusión y ejecución de la presente orden en materia de seguridad interior y en coordinación con la Agencia Digital de Andalucía en materia de política de seguridad de la información.

Disposición final segunda. Publicidad de la política de seguridad de la Consejería.

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 web y medios de difusión internos (Intranet) de la Consejería y sus entes instrumentales y en la sección de transparencia del Portal de la Junta de Andalucía, sin perjuicio de las obligaciones previstas en el artículo 13 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía y en los medios y soportes que se establezcan por el Comité de Seguridad Interior y Seguridad TIC.

Disposición final tercera. Entrada en vigor.

La presente orden entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Junta de Andalucía.

Sevilla, 15 de noviembre de 2023

CARLOS ARTURO BERNAL BERGUA
Consejero de Turismo, Cultura y Deporte

00293147