3. Otras disposiciones

CONSEJERÍA DE UNIVERSIDAD, INVESTIGACIÓN E INNOVACIÓN

Orden de 8 de mayo de 2024, por la que se establece la política de seguridad interior y seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería de Universidad, Investigación e Innovación y de sus entidades adscritas.

Mediante Orden de 12 de julio de 2019, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas, de acuerdo con lo establecido en el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se define la política de seguridad de las tecnologías de la información y comunicaciones (en adelante, TIC) de la Consejería de Economía, Conocimiento, Empresas y Universidad, que se ha de aplicar en el tratamiento de los activos TIC de su titularidad o cuya gestión tenga encomendada, y se crea el Comité de Seguridad TIC, como órgano regulado en 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 en la Administración de la Junta de Andalucía, para la dirección y seguimiento en materia de seguridad de los activos TIC de dicha Consejería.

En esta misma orden se definen además los objetivos y criterios básicos para el tratamiento de la política de seguridad, concretando el contenido de ese marco normativo de seguridad en esta Consejería y la estructura organizativa y de gestión que velaría por su cumplimiento.

Con la aprobación y entrada en vigor del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, la disposición final primera modifica de forma expresa el Decreto 1/2011, de 11 de enero, indicando que todas las alusiones en el texto a los «Comités de Seguridad TIC de las entidades» quedarían sustituidas por «Comités de Seguridad Interior y Seguridad TIC de Consejerías o entidades dependientes singulares».

Por otra parte, el artículo 9 del Decreto 171/2020, de 13 de octubre, establece respecto a las normas de creación de dichos Comités de Seguridad Interior y Seguridad TIC, que modificarán su denominación añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior, actualizando su composición y régimen de los mismos, con descripción incluso de las nuevas funciones a incorporar.

En virtud de lo expuesto, y atendiendo a los principios de simplificación, economía, eficacia y eficiencia administrativa, se hizo necesaria la aprobación de la Orden de 4 de abril de 2022, por la que se modifica la de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.

Con el Decreto del Presidente 10/2022, de 25 de julio, sobre reestructuración de Consejerías, se crea la Consejería de Universidad, Investigación e Innovación. El Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la misma establece en su disposición transitoria cuarta que, en tanto esta Consejería no disponga de una política propia de seguridad TIC, de acuerdo con lo previsto en el artículo 10 del Decreto 1/2011, de 11 de enero, será de aplicación la establecida en la Orden de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad.

En este sentido, y de acuerdo con el artículo 17 de la Orden de 12 de julio de 2019, con fecha 26 de mayo de 2023 se convoca el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación, que acuerda el inicio de una nueva orden por la que se establezca la política de seguridad interior y seguridad de

00301588

las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.

Por otra parte, de acuerdo con lo establecido en el artículo 5 de la Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía, esta norma integra el principio de igualdad de género de forma transversal en su elaboración, garantizando con ello un impacto positivo en la igualdad de oportunidades entre mujeres y hombres.

En la elaboración y tramitación de la presente orden, se ha actuado conforme a los principios de buena regulación a los que se refiere el artículo 129.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En cuanto a los principios de necesidad y eficacia, la orden no hace sino cumplir con el mandato del Decreto 171/2020, de 13 de octubre, siendo necesaria su adecuación; cumple con el de proporcionalidad al desarrollar estrictamente el mandato del Decreto, no imponiendo más obligaciones a la ciudadanía ni a la Administración que los establecidos en él y regulando figuras necesarias para el cumplimiento de la finalidad perseguida; sobre el de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación; acerca del de transparencia, al tratarse de una disposición de organización interna no ha habido consulta previa ni trámite de audiencia a la ciudadanía, limitándose los informes a los internos de la Administración; y, es eficiente porque no solo evita imponer cargas administrativas adicionales, sino que se limita a utilizar los recursos ya existentes para prestar los servicios requeridos sin que suponga ningún incremento de gasto.

En su virtud, a propuesta de la Secretaría General Técnica, de acuerdo con lo dispuesto en el artículo 26.2.a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía; los artículos 44.2 y 46.4 de la Ley 6/2006, de 24 de octubre, de Gobierno de la Comunidad Autónoma de Andalucía, en el Decreto del Presidente 10/2022, de 25 de julio, sobre reestructuración de Consejerías, y en el Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la Consejería de Universidad, Investigación e Innovación,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

Es objeto de la presente orden la regulación, en el ámbito de la Consejería de Universidad, Investigación e Innovación de:

a) Establecer la política de seguridad interior de la Consejería de Universidad, Investigación e Innovación (en adelante la Consejería) que defina el sistema para la prevención y reacción ante daños intencionadamente provocados por agentes externos, personal propio o personas usuarias, contra sus propias personas usuarias, su personal, sus activos y la continuidad de su funcionamiento y servicios.

b) Definir y regular la política de seguridad de las tecnologías de la información y las comunicaciones (en adelante, seguridad TIC) de esta Consejería, y constituye su documento de política de seguridad TIC.

c) La protección de datos personales.

Artículo 2. Ámbito de aplicación.

1. En materia de política de seguridad interior, la presente orden será de aplicación al conjunto de los activos en el ámbito de la Consejería, de conformidad con lo dispuesto

00301588

en el Decreto 158/2022, de 9 de agosto, por el que se regula la estructura orgánica de la Consejería de Universidad, Investigación e Innovación.

2. En materia de seguridad TIC, la presente orden será de aplicación, además de a los órganos directivos centrales y periféricos de la Consejería, a las entidades vinculadas o dependientes que se encuentren adscritas orgánicamente a la misma, de acuerdo con el artículo 2.3 del Decreto 158/2022, de 9 de agosto.

3. En materia de protección de datos, también será de aplicación para todo el personal que acceda tanto a los sistemas de información como a la propia información, ya sea en formato electrónico o en papel, que sea gestionada por la Consejería, con independencia de cuál sea el destino, adscripción o relación con la misma.

Artículo 3. Marco regulador.

El marco regulador en materia de seguridad interior está constituido por lo previsto en el artículo 15 del Decreto 171/2020, de 13 de octubre, por el que se establece la política de seguridad interior en la Administración de la Junta de Andalucía, y en materia de seguridad TIC se atenderá a lo dispuesto por la disposición adicional primera del Decreto 1/2011, de 11 enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Asimismo, será de aplicación 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, 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 en materia de protección de datos.

Artículo 4. Definiciones, objetivos y principios.

1. Los objetivos y principios básicos de la política de seguridad interior son los establecidos en los artículos 4 y 5 del Decreto 171/2020, de 13 de octubre.

2. Las definiciones, los objetivos y los principios de la política de seguridad TIC son los establecidos en los artículos 2, 4 y 5, así como en el Glosario de Términos incluido como Anexo I del Decreto 1/2011, de 11 de enero.

CAPÍTULO II

Política de seguridad interior y seguridad TIC

Artículo 5. Contexto.

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

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

Artículo 6. Obligaciones generales.

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

00301588

2. A los sistemas de información que traten datos personales se aplicará lo dispuesto en la normativa vigente en materia de protección de datos, así como las recomendaciones y directrices dictadas por el Consejo de Transparencia y Protección de Datos de Andalucía, en materia de protección de datos.

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

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos. En los supuestos de sistemas de información que traten datos personales se realizará, con el asesoramiento del delegado de protección de datos, un análisis de riesgos conforme al artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y, en los supuestos de su artículo 35, una evaluación de impacto relativa a la protección de datos.

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

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

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

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

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

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

i) Integridad y actualización del sistema. Se requerirá una autorización formal previa a la instalación de un sistema por parte de la persona responsable del servicio de acuerdo con lo dispuesto en el artículo 18 de esta orden. Se deberá conocer el estado de la seguridad del sistema en relación con las recomendaciones y actualizaciones de seguridad recomendadas por el fabricante.

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

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

l) Registro de actividad y detección de código dañino. Se registrarán aquellos eventos que se consideren de interés, tanto para la detección de actividades que puedan comprometer la seguridad, como para dejar constancia de aquellas otras actividades que

00301588

permitan verificar y evidenciar la efectividad de los controles, las normas de seguridad establecidas por la Consejería y los requisitos legales aplicables.

m) Incidentes de seguridad.

n) Continuidad de la actividad. Las personas responsables del servicio de acuerdo con el artículo 18, deberán elaborar planes de continuidad del negocio. Se implantarán mecanismos apropiados para asegurar la disponibilidad de los sistemas de información teniendo en cuenta la valoración de la dimensión de disponibilidad.

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

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

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

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

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

Artículo 7. Prevención.

1. Las unidades organizativas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS y 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.

2. Los controles, los perfiles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

3. Para garantizar el cumplimiento de la política, las unidades organizativas deben:

a) Autorizar la puesta en funcionamiento de los sistemas TIC de su competencia.

b) Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

c) Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Artículo 8. Detección.

1. Se monitorizará de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el ENS, para evitar su rápida degradación debido a incidentes.

Si la anomalía detectada afectase a datos personales, se contactará con el responsable del tratamiento que actuará de acuerdo con lo establecido en el artículo 40 de la presente orden, relativo a la violación de la seguridad de los datos personales.

2. La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con lo dispuesto en el ENS. Así, se establecerán mecanismos de

00301588

detección, análisis y reporte que lleguen a las personas responsables tanto de una manera regular, como cuando se produzca alguna desviación significativa de los parámetros que se hayan preestablecido como normales.

Artículo 9. Respuesta.

Las unidades organizativas deben:

a) Colaborar con el equipo de gestión de incidentes de seguridad de la Consejería y con el delegado de protección de datos, en caso de que se vean afectados datos personales.

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

c) Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los equipos de respuesta ante emergencias informáticas.

Artículo 10. Recuperación.

Para garantizar la disponibilidad de los servicios críticos, las personas responsables del servicio deben colaborar en el desarrollo de planes de continuidad de sus sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación liderados por el Comité de Seguridad Interior y Seguridad TIC.

Artículo 11. Planificación de las actividades para la seguridad interior contra riesgos intencionales.

1. La planificación de las actividades para la seguridad interior contra riesgos intencionales en el ámbito de la Consejería se realizará mediante un Plan de Seguridad Interior de la Consejería, aprobado por el Comité de Seguridad Interior y Seguridad TIC a propuesta de la correspondiente Unidad de Seguridad Interior y que, como mínimo, comprenderá:

a) La identificación de todo el personal de la Consejería implicado en la organización de la Seguridad Interior, con previsiones sobre la frecuencia y mecanismos de comunicación y escalado de informaciones.

b) La relación de normas y procedimientos para la seguridad interior de común aplicación a su ámbito.

c) La determinación de activos-tipo en el ámbito de su Consejería o entidad.

d) El análisis de riesgos para sus activos-tipo.

e) Los niveles de protección objetivo para sus activos-tipo.

f) Los tipos de medidas de seguridad pertinentes para los riesgos-tipo en los activos de su ámbito.

g) Los criterios de priorización de gastos e inversiones en la seguridad interior de los activos de su ámbito y previsión para los próximos ejercicios.

2. Por cada activo (o clase de personal, o de personas usuarias) singular en virtud de su volumen o tipo especial de riesgos, según apreciación del Comité y a propuesta de la Unidad de Seguridad Interior, se realizará un plan, propuesto por quien identificó la necesidad y aprobado por quien la apreció, y que, como mínimo, comprenderá:

a) La descripción del activo y sus elementos.

b) La identificación de todo el personal que está implicado en la organización de la Seguridad Interior, con previsiones sobre la frecuencia y mecanismos de comunicación y escalado de informaciones.

c) La identificación de amenazas.

d) La identificación de riesgos.

e) El nivel de riesgo inherente.

f) Las medidas de seguridad existentes.

g) La estimación del nivel de protección objetivo del activo.

h) Las medidas a adoptar incluyendo, en su caso, previsiones de gasto e inversión.

00301588

i) El programa de implantación.
j) Las previsiones para la revisión continua del plan.

3. La planificación de las actividades para la seguridad interior contra riesgos intencionales se realizará con especial atención a lo previsto en la normativa sobre protección de datos personales. Al respecto, el plan incorporará una memoria relativa a la aplicación del principio de responsabilidad proactiva y protección desde el diseño, así como un informe del correspondiente delegado de protección de datos.

Artículo 12. Estructura organizativa de la seguridad interior y seguridad TIC.

La estructura organizativa de la seguridad interior y seguridad TIC se distribuye en dos niveles:

a) En la Consejería de Universidad, Investigación e Innovación:
1.º Comité de Seguridad Interior y Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La Unidad de Seguridad TIC.
5.º La Unidad de Seguridad Interior.
6.º La persona responsable de seguridad TIC.
7.º Las personas responsables del sistema.

Además, de conformidad con lo establecido en la normativa sobre protección de datos personales, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas con la seguridad TIC:
8.º La figura del responsable del tratamiento.
9.º La figura del encargado del tratamiento.

b) En cada una de las entidades vinculadas o dependientes:
1.º Comité de Seguridad Interior y Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La persona responsable de seguridad TIC.
5.º Las personas responsables del sistema.
6.º La Unidad de seguridad Interior en caso de que se constituya en aquellas entidades dependientes en las que estas lo consideren necesario por virtud del volumen o singularidad de los activos.

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

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

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

Artículo 13. Creación y composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Universidad, Investigación e Innovación.

1. Se crea el Comité de Seguridad Interior y Seguridad TIC de la Consejería como unidad administrativa especial para la dirección y seguimiento en materia de seguridad interior en todos sus ámbitos de actuación y en materia de seguridad de los activos TIC de los que dicha Consejería sea titular o cuya gestión tenga encomendada.

2. El Comité de Seguridad Interior y Seguridad TIC de la Consejería estará compuesto por los siguientes miembros:

00301588

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

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 tengan atribuidas funciones y tareas relacionadas con la custodia y la seguridad de los activos adscritos a la Consejería o sobre algún sistema de información.

2º. La persona titular de la coordinación general de la Viceconsejería.

3.º La persona titular de la coordinación general de la Secretaría General Técnica.

4.º El delegado de protección de datos.

5.º La persona responsable de seguridad TIC.

6.º La persona responsable de seguridad interior.

d) Secretaría: La persona titular de la Jefatura de Sistemas de Información Sectoriales de Innovación y Sostenibilidad, con voz y voto.

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

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

Artículo 14. Funciones del Comité de Seguridad Interior y Seguridad TIC.

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

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

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

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

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

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

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

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

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

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

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

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

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

00301588

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

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

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

e) Nombrar a la persona responsable de seguridad TIC.

f) Nombrar a las personas responsables del sistema.

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

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

i) Informar regularmente a la persona titular de la Consejería del estado de la seguridad de las TIC en su ámbito.

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

k) Aprobar las normas generales de seguridad TIC, además de la normativa de segundo nivel de seguridad TIC de la Consejería.

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

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

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

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

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

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

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

r) Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos, velando, en particular, por la coordinación en la gestión de incidentes de la seguridad TIC y por los riesgos que pudiera suponer para los datos personales.

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

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

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

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

00301588

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

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

y) Coordinar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, de acuerdo con el correspondiente análisis de riesgo para los derechos y libertades de las personas físicas y, en su caso, las evaluaciones de impacto relativas a la protección de datos personales, contando con el asesoramiento del delegado de protección de datos.

Artículo 15. Funcionamiento del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC se reunirá con carácter ordinario, al menos, una vez al año y, con carácter extraordinario, cuando lo decida la persona titular de la presidencia, de oficio o a propuesta de alguno de sus miembros, y en todo caso cuando se produzca alguno de los siguientes supuestos:

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

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

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

Los miembros del Comité de Seguridad Interior y Seguridad TIC están obligados a respetar la confidencialidad de toda la información a la que tengan acceso.

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

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

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

6. En todo lo no previsto le será de aplicación lo establecido en la sección tercera de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 16. Perfiles de responsabilidad.

Las figuras o perfiles de responsabilidad en el ámbito de esta orden se definen como un conjunto de responsabilidades y atribuciones que deben quedar adecuadamente cubiertas dentro de la organización, con los perfiles idóneos y con independencia de a qué persona concreta o conjunto de personas sean asignadas, cumpliendo, en cualquier caso, el principio de función diferenciada establecido tanto en el ENS como en la política de seguridad TIC de la Junta de Andalucía.

00301588

Artículo 17. Responsable de la información.

1. La figura de responsable de la información en lo relativo al ENS, será aquella persona titular de centro directivo que tiene la responsabilidad sobre la información y determina sus niveles de seguridad dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, siendo posible la presentación de una propuesta previa por parte del Comité de Seguridad Interior y Seguridad TIC. Esta persona mantendrá dicha condición mientras conserve la titularidad del centro directivo.

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

La persona responsable de la información tendrá la condición de responsable del tratamiento, definida en el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, salvo que las normas aplicables sobre asignación de atribuciones en materia de protección de datos personales dispongan de otra cosa.

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

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

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

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

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

4. La persona responsable del servicio conservará su condición mientras ostenten el cargo que haya determinado su nombramiento.

Artículo 18. Responsable del servicio.

1. La figura de responsable del servicio, en lo relativo al ENS, es el agente que determinará los niveles de seguridad de los servicios dentro del marco establecido en el Anexo I del Real Decreto 311/2022, de 3 de mayo.

La figura de responsable del servicio corresponderá a las personas titulares de cada órgano directivo o unidad administrativa, al menos con nivel de jefatura de servicio y mantendrá dicha condición mientras conserven dicha titularidad.

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

a) Ayudar a determinar los requisitos de seguridad de los servicios a prestar, identificando los niveles de seguridad de los mismos mediante la valoración del impacto sobre éstos de los incidentes que pudieran producirse.

b) En el ámbito de cada servicio, proporcionar la información necesaria a la Unidad Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de

00301588

establecer las salvaguardas a implantar. Para ello, contará con la ayuda de la persona responsable del sistema.

Artículo 19. Unidad de Seguridad Interior.

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

La Unidad de Seguridad Interior de la Consejería tendrá las siguientes funciones:

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

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

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

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

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

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

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

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

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

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

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

l) Asegurar en el ámbito de la Consejería, el funcionamiento de los mecanismos previstos para recopilar, recibir, analizar y procesar la información relevante para la seguridad interior, destinados a generar inteligencia al respecto. En la medida en que los mecanismos citados impliquen un tratamiento de datos personales, deberá explicitarse el mismo, recoger sus elementos principales y determinar las medidas técnicas y organizativas adecuadas para garantizar el cumplimiento en materia de protección de datos.

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

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

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

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

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

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

00301588

Artículo 20. Unidad de Seguridad TIC.

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

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

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

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

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

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

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

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

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

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

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

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

Artículo 21. Responsable de seguridad TIC.

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

a) Dirigirá la Unidad de Seguridad TIC de la Consejería.

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

c) Será responsable de:

00301588

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

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

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

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

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

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

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

Estas funciones se desempeñarán con el asesoramiento del delegado de protección de datos, de acuerdo con el artículo 3.2 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y con el contenido de los requisitos de protección de la información sobre datos personales contemplado en el apartado 5.7.1 del Anexo II de dicho real decreto.

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

e) Aprobar las normas de tercer nivel.

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

Artículo 22. Responsable del sistema.

1. En virtud del artículo 10.4 del Decreto 1/2011, de 11 de enero, la presente política establece que los deberes y responsabilidades de este perfil de responsabilidad serán los previstos en el ENS y la guía CCN-STIC-801 para la figura del responsable del sistema, y su designación, nombramiento y renovación se adoptará por decisión del Comité de Seguridad Interior y Seguridad TIC y se comunicará a la persona interesada.

2. Desde la perspectiva del ENS, la figura del responsable a que se refiere este artículo, respecto de los sistemas de información cuya implantación, explotación y mantenimiento se haga fuera de la Consejería (en otros organismos de la Junta de Andalucía o en empresas externas) será nombrada o renovada por la persona responsable de la información o la persona responsable del servicio correspondiente. El nombramiento y cese, en todo caso, será comunicado a la persona afectada.

3. Las personas responsables del sistema serán nombradas por el Comité de Seguridad Interior y Seguridad TIC que corresponda, y tendrá las siguientes atribuciones:

a) Gestionar el sistema durante todo su ciclo de vida, desde la especificación, la instalación, hasta el seguimiento de su funcionamiento.

00301588

b) Definir los criterios de uso y los servicios disponibles en el sistema.

c) Elaborar los procedimientos operativos de seguridad para su aprobación por la persona responsable de seguridad TIC.

d) Determinar la configuración autorizada de hardware y software a utilizar en el sistema y aprobar las modificaciones importantes de dicha configuración.

e) Implantar y controlar las medidas específicas de seguridad del sistema.

f) Elaborar, junto con la persona responsable de seguridad TIC, los planes de mejora continua de la seguridad que deberá aprobar el Comité de Seguridad Interior y Seguridad TIC.

g) Elaborar planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

h) Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada, del servicio afectado y la persona responsable de seguridad TIC, antes de ser ejecutada.

Artículo 23. Entidades vinculadas o dependientes.

1. De acuerdo con lo dispuesto en el artículo 10 del Decreto 1/2011, de 11 de enero, cada entidad deberá contar con un documento de política de seguridad TIC, que será aprobado por la persona titular de la entidad correspondiente y se plasmará en los términos descritos en el Real Decreto 311/2022, de 3 de mayo, sin perjuicio de lo establecido en el artículo 10.3 del Decreto 1/2011, de 11 de enero, en el que se indica que el documento de política de seguridad TIC de las Consejerías y sus documentos complementarios también serán de obligado cumplimiento para sus entidades vinculadas o dependientes.

2. Cada entidad vinculada o dependiente deberá contar con un Comité de Seguridad Interior y Seguridad TIC de los regulados en el artículo 10 del Decreto 1/2011, de 11 de enero, que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada. Las atribuciones de los Comités de Seguridad Interior y Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por los comités de dirección existentes en dichas entidades, circunstancia que deberá ser recogida expresamente en el correspondiente documento de política de seguridad TIC.

3. El documento de política de seguridad TIC de las entidades vinculadas o dependientes, deberá recoger la composición, atribuciones y funcionamiento del Comité de Seguridad Interior y Seguridad TIC y del resto de perfiles con responsabilidad en seguridad, incluyendo, en su caso, los recogidos en el Real Decreto 311/2022, de 3 de mayo, definiendo, para cada uno de ellos, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

4. El Comité de Seguridad Interior y Seguridad TIC de la Consejería articulará los protocolos comunes de colaboración y coordinación necesarios con los comités de sus entidades vinculadas o dependientes.

5. Las entidades vinculadas o dependientes contarán, al menos, con una persona responsable de seguridad TIC que será nombrada por el Comité de Seguridad Interior y Seguridad TIC de las mismas y que tendrá las atribuciones que establece el artículo 11.2 del Decreto 1/2011, de 11 de enero.

Artículo 24. Actualización de la política de seguridad de la información.

Una de las funciones del Comité de Seguridad Interior y Seguridad TIC de la Consejería consistirá en la revisión anual de esta política de seguridad de la información y la propuesta de revisión o mantenimiento de la misma. Las modificaciones en la política de seguridad serán aprobadas por la persona titular de la Consejería y difundidas a través

00301588

de los medios que se establezcan por el Comité de Seguridad Interior y Seguridad TIC, sin perjuicio de su publicación en el Boletín Oficial de la Junta de Andalucía.

Artículo 25. Gestión de riesgos.

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

En los supuestos de sistemas de información que traten datos personales, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

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

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

Artículo 26. Responsabilidades en la gestión de riesgos.

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

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

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

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

Artículo 27. Análisis de riesgos.

1. El análisis de riesgos se realizará, al menos, una vez al año por parte de la Unidad de Seguridad TIC. Además se producirá un análisis de riesgos cuando se produzcan los siguientes supuestos:

a) Cuando cambie la información manejada.

b) En el momento en que se modifiquen los servicios prestados.

c) En el tiempo en que ocurra un incidente grave de seguridad.

d) Cuando se detecten vulnerabilidades graves.

e) Cuando se determine de forma motivada por el Comité de Seguridad Interior y Seguridad TIC.

2. La Unidad de Seguridad TIC elevará el informe correspondiente al análisis realizado al Comité de Seguridad Interior y Seguridad TIC.

00301588

3. Para realizar el análisis de riesgos se utilizarán las metodologías y las herramientas que apliquen, de acuerdo con lo establecido en el ENS.

4. Para la armonización de los análisis de riesgos, el Comité de Seguridad Interior y Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad Interior y Seguridad TIC propiciará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Artículo 28. Categorización de los sistemas.

La determinación de la categoría de un sistema se realizará de acuerdo a lo que el ENS establezca al respecto.

Artículo 29. Desarrollo normativo de la política de seguridad de la información.

1. El cuerpo normativo sobre seguridad TIC es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: Política de seguridad TIC, directrices y normas generales de seguridad TIC.

b) Segundo nivel normativo: Normas específicas de seguridad TIC, que desarrollan y detallan la política de seguridad TIC, centrándose en un área o aspecto determinado.

c) Tercer nivel normativo: Procedimientos, procesos, guías e instrucciones técnicas de seguridad TIC, que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la política de seguridad TIC.

2. Además de los documentos citados en el apartado anterior, la documentación de seguridad TIC de los órganos contemplados en el ámbito de aplicación de esta norma podrá contar, bajo criterio de la Unidad de Seguridad TIC, con otros documentos de carácter no vinculante como pueden ser: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, y otros establecidos al respecto.

3. La Unidad de Seguridad TIC, deberá mantener la documentación de seguridad actualizada y organizada, así como gestionar los mecanismos de acceso a la misma.

4. El Comité de Seguridad Interior y Seguridad TIC establecerá los mecanismos necesarios para publicar y compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la política de seguridad TIC.

Artículo 30. Gestión de incidentes de seguridad y de la continuidad.

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

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

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

00301588

Artículo 31. Concienciación y formación. Obligaciones del personal.

1. La seguridad de la información afecta a todas las personas que prestan servicios en la Consejería y a todas las actividades, de acuerdo con el principio de seguridad integral recogido en el artículo 6 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. El objetivo consiste en lograr la plena conciencia de estas personas, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que pueden acaecer. Adicionalmente, las personas con responsabilidad en el uso, operación y administración de sistemas TIC deberán haber recibido formación en el manejo seguro de los sistemas, en la medida en que la necesiten para realizar sus funciones.

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

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

Artículo 32. Terceras partes.

1. En los supuestos de colaboración de la Consejería con otras entidades o departamentos, o maneje información de estos, se les hará partícipes de esta política de seguridad TIC, estableciéndose canales para la comunicación y coordinación de los respectivos Comités de Seguridad Interior y Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad y violaciones de seguridad de los datos personales.

2. Cuando la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que ataña a estos servicios o información. Los terceros quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias, y violaciones de seguridad de los datos personales, así como se garantizará que el personal correspondiente a dicha tercera parte esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política de seguridad TIC. Los terceros cuyos servicios sean utilizados por la Consejería o a los que ésta les ceda o comunique información estarán sujetos al deber de confidencialidad de acuerdo con el artículo 5.1 de la Ley Orgánica 3/2018, de 5 de diciembre, en relación con el artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

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

Artículo 33. Auditorías y conformidad normativa.

1. La Consejería auditará los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo vigente, así como el cumplimiento en materia de protección de datos, en aquellos sistemas de información que traten datos personales.

2. Los sistemas de información de la Consejería serán objeto, al menos, cada dos años, de una auditoría regular ordinaria interna o externa que verifique el cumplimiento de

00301588

los requisitos del ENS y de cualquier otra norma que requiera la realización de auditorías periódicas. La Unidad de Seguridad TIC coordinará estas actividades de auditoría, y analizará y elevará a la persona responsable de seguridad TIC, a la persona responsable del sistema y al delegado de protección de datos si las conclusiones afectan a los datos personales. La persona responsable del sistema adoptará las medidas correctoras adecuadas. Si las conclusiones requieren, a priori, un cambio normativo, deberán elevarse al Comité de Seguridad Interior y Seguridad TIC para que adopte las medidas adecuadas.

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

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

Artículo 34. Cooperación con otros órganos y otras Administraciones en materia de seguridad.

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 el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

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

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

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

d) La 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 del Estado, la Administración autonómica y las Entidades que integran la Administración Local.

e) La Agencia Española de Protección de Datos.

f) El Instituto Nacional de Ciberseguridad.

g) El Grupo de Delitos Telemáticos 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.

Artículo 35. Resolución de conflictos.

1. En caso de conflicto entre los diferentes responsables, este será resuelto por el órgano superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad Interior y Seguridad TIC.

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

Artículo 36. Difusión de la política de seguridad de la información.

A los efectos de su mejor difusión entre el personal de la organización y de otras partes interesadas, la presente política de seguridad TIC 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 Interior y Seguridad TIC.

CAPÍTULO III

Protección de datos personales

Artículo 37. Protección de datos personales.

1. Todos los sistemas de información de la Consejería y de sus entidades vinculadas o dependientes, se ajustarán a lo exigido por el Reglamento (UE) 2016/679 del Parlamento

00301588

Europeo y del Consejo de 27 de abril de 2016, la Ley Orgánica 3/2018, de 5 de diciembre, y por el resto de la normativa general o sectorial de protección de datos personales que sea de aplicación.

2. Todos los tratamientos de datos personales, automatizados o no automatizados, se sujetarán a la citada normativa cuando se encuentren dentro de su ámbito de aplicación.

Artículo 38. Medidas técnicas y organizativas.

1. Las medidas técnicas y organizativas a implantar tendrán en cuenta lo previsto en el artículo 13.h) de la Ley 39/2015, de 1 de octubre, que reconoce a las personas, en sus relaciones con las Administraciones Públicas, el derecho a la protección de 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.

2. Las personas responsables del tratamiento en el ámbito de aplicación de esta orden, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades de las personas físicas, que serán revisadas regularmente, de conformidad con el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

3. Todas las personas, físicas o jurídicas, que actúen bajo la autoridad del responsable de un tratamiento estarán sujetas al principio de confidencialidad previsto en el artículo 5.1.f) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y en el artículo 5.1 de la Ley Orgánica 3/2018, de 5 de diciembre. Dicho deber se extiende aún después de finalizada la relación del obligado con dicho responsable del tratamiento, de acuerdo con el artículo 5.3 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 39. Evaluación de impacto.

1. 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, de conformidad con el artículo 35 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

2. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos análogos. Para ello, recabará el asesoramiento de la persona delegada de protección de datos.

Artículo 40. Registro de actividades de tratamiento.

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

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

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

Artículo 41. Violación de la seguridad de los datos personales.

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento lo pondrá en conocimiento del delegado o delegada de protección de datos,

00301588

efectuará la valoración del riesgo que la misma suponga para los derechos y libertades de las personas físicas, y la notificará al Consejo de Transparencia y Protección de Datos de Andalucía sin dilación indebida y, con un plazo máximo de 72 horas posteriores a computar desde que haya tenido constancia de ella, salvo que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en dicho plazo máximo, esta deberá ir acompañada de la indicación de los motivos de la dilación.

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

Todo ello de acuerdo con lo establecido en los artículos 33 y 34 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y en el resto de la normativa de datos personales aplicable.

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

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

Artículo 42. Delegado de protección de datos personales.

1. El delegado de protección de datos personales será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos, de conformidad con lo establecido en los artículos 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre. En la designación deberá especificarse el alcance de la misma, indicando los responsables de tratamiento para los que ejercerá sus funciones.

2. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, de acuerdo con el artículo 38.3 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.

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

Artículo 43. Los delegados de protección de datos personales en las entidades vinculadas o dependientes.

La dirección de cada entidad vinculada o dependiente deberá nombrar un delegado de protección de datos personales que se comunicará al Consejo de Transparencia y Protección de Datos de Andalucía y al Comité de Seguridad Interior y Seguridad TIC de la Consejería. El delegado de protección de datos será designado de acuerdo con lo previsto en el 41.1 de la presente orden.

Artículo 44. Responsables del tratamiento de datos personales.

Los responsables del tratamiento de datos personales en el ámbito de aplicación de esta orden son los órganos directivos que determinen los fines y medios de los tratamientos, de conformidad con el artículo 4.7 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

00301588

Artículo 45. Encargados del tratamiento de datos personales.

1. De conformidad con el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 cuando se vayan a tratar datos personales por cuenta de un responsable, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento garantice la protección de los derechos del interesado. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico constará por escrito, inclusive en formato electrónico.

2. Las principales funciones y responsabilidades, dentro de su ámbito de actuación, son las establecidas en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y demás normativa de aplicación.

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

Disposición adicional única. Constitución del Comité de Seguridad Interior y Seguridad TIC.

La primera reunión del Comité de Seguridad Interior y Seguridad TIC tendrá por objeto la constitución del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente orden.

Disposición derogatoria única. Derogación de normas.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden y en particular la Orden de 12 de julio de 2019, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas, en lo que afecte al ámbito de esta Consejería.

Disposición final primera. Habilitación para ejecución.

Se habilita a la persona titular de Secretaría General Técnica para dictar cuantas actuaciones sean necesarias para la ejecución de lo establecido en la presente orden.

Disposición final segunda. 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, 8 de mayo de 2024

JOSÉ CARLOS GÓMEZ VILLAMANDOS
Consejero de Universidad, Investigación e Innovación

00301588