3. Otras disposiciones

CONSEJERÍA DE TRANSFORMACIÓN ECONÓMICA, INDUSTRIA, CONOCIMIENTO Y UNIVERSIDADES

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.

El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.º atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

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, define y regula la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, conformando, junto a las disposiciones y documentos técnicos que la desarrollen, el marco regulador de seguridad TIC.

El artículo 10 del citado decreto dispone que cada Consejería y Entidad incluida en su ámbito de aplicación deberá disponer de un Comité de Seguridad TIC, como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Por otra parte, en un escenario general en el que los riesgos de daños intencionales se multiplican, se hacía inaplazable abordar como objetivo la explícita definición de un sistema de seguridad interior de la Administración de la Junta de Andalucía para la prevención y reacción ante daños en las personas, el patrimonio y el funcionamiento, intencionadamente provocados por agentes externos, personal propio o usuarios.

Así, 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, tiene por objeto implantar una política de seguridad interior que defina un completo 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. De esta forma, la Administración de la Junta de Andalucía despliega en todos sus ámbitos de actuación una notable actividad relacionada con la vigilancia y la protección ante posibles riesgos intencionales. Este decreto responde, asimismo, a la necesidad de solventar un déficit de planificación y organización que impedía asegurar que tales recursos se estuvieran gestionando con los máximos niveles de eficacia y eficiencia.

En este decreto, además, atendiendo a principios de simplificación, economía, eficacia y eficiencia administrativa se ha optado por evitar la creación ex-novo de un comité para la seguridad interior en cada Consejería o entidad, optando por incluir las que hubieran sido sus funciones y tareas entre las de los actuales Comités de Seguridad TIC, previamente creados de acuerdo con la normativa anteriormente citada. De esta forma, el artículo 9 del Decreto 171/2020, de 13 de octubre, dispone que, en cada Consejería o entidad dependiente, existirá un Comité de Seguridad Interior y Seguridad TIC, debiendo las normas de creación de los Comités a los que alude el artículo 10 del Decreto 1/2011, de 11 de enero, modificar su denominación y actualizar, de ser necesario, la composición y régimen de los mismos, con descripción incluso, de las nuevas funciones a incorporar.

00259662

Mediante Orden de 12 de julio de 2019, de la Consejería de Economía, Conocimiento, Empresas y Universidad, se definió y reguló la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de esta Consejería y de sus entidades adscritas. De esta forma, se impulsó que las tecnologías de la información y comunicaciones fuesen administradas con diligencia, adoptando las medidas adecuadas para protegerlas frente a daños accidentales o deliberados que pudieran afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados. Asimismo, se creó el Comité de Seguridad TIC de la Consejería y se estableció, a su vez, su composición y funciones.

Vistos los antecedentes mencionados, la modificación que se plantea de la Orden de 12 de julio de 2019, se basa, fundamentalmente, de un lado, en introducir cambios en su estructura organizativa para incluir los relativos al ámbito de la seguridad interior. Esta solución organizativa supone además un nuevo avance en la coordinación entre la seguridad física y la ciberseguridad, favoreciendo las sinergias posibles entre ambas materias.

De otro lado, la modificación se refiere específicamente al ámbito de seguridad TIC y, en primer lugar, responde al cumplimiento de determinadas recomendaciones del informe de la auditoría de que ha sido objeto recientemente nuestra Consejería, cuya consecuencia ha sido la obtención del certificado de adecuación al Esquema Nacional de Seguridad (ENS) de los sistemas de nivel de seguridad medio. Las citadas recomendaciones implican la modificación de algunos aspectos formales de la política de seguridad TIC, que han sido recogidas íntegramente en el nuevo texto. En segundo lugar, consecuencia de la experiencia adquirida en el funcionamiento del Comité de Seguridad TIC, se plantea, más justificado si cabe al dotársele de nuevas competencias en materia de seguridad interior, un cambio en la frecuencia mínima anual de celebración de sus reuniones ordinarias, otorgando una mayor relevancia a la celebración de reuniones extraordinarias cuando la necesidad lo requiera, en aras de una mayor eficacia y eficiencia.

Por último, se introducen una serie de modificaciones que tienen por objeto fundamental actualizar la orden conforme a la regulación actual en materia de protección de datos. En este sentido, se especifican las obligaciones formales de los responsables del tratamiento de datos personales para mayor seguridad jurídica. Así, en cuanto a la publicación de su Registro de Actividades de Tratamiento en el Inventario, como en lo referido a la necesidad de la constancia de un contrato u otro acto jurídico por escrito que legitime el tratamiento de datos personales por un encargado por cuenta del responsable. También se determina el protocolo a seguir para la resolución y notificación en caso de violaciones de seguridad.

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 esta 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, así como el artículo 7 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía. En cuanto a los principios de necesidad y eficacia, la orden da cumplimiento a lo establecido el artículo 9 del Decreto 171/2020, de 13 de octubre; cumple con el de proporcionalidad al desarrollar el mandato del citado 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. Asimismo, respeta los principios de eficiencia y transparencia, por cuanto

00259662

favorece la racionalización de la estructura organizativa y el funcionamiento de la Administración de la Junta de Andalucía, a la vez que permite su conocimiento por parte de la ciudadanía. Asimismo se han tenido también en cuenta los principios generales de organización y funcionamiento de la Administración de la Junta de Andalucía, establecidos en el artículo 3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

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, del Gobierno de la Comunidad Autónoma de Andalucía, en el Decreto del Presidente 3/2020, de 3 de septiembre, de la Vicepresidencia y sobre reestructuración de Consejerías, y en el Decreto 117/2020, de 8 de septiembre, por el que se regula la estructura orgánica de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades,

D I S P O N G O

Artículo único. Modificación de la Orden 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.

Se modifica la Orden 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, en los siguientes términos:

Uno. Se añade un segundo párrafo al apartado 1 del artículo 1, que queda redactado como sigue:

«Asimismo, de conformidad con lo establecido en el artículo 9 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 presente orden tiene por objeto definir y regular la política de seguridad interior de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades 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.»

Dos. Se añade un apartado 3 al artículo 3, que queda redactado como sigue:

«3. De acuerdo con lo establecido en el artículo 1 del Decreto 171/2020, de 13 de octubre, la presente Orden será de aplicación a la seguridad interior del conjunto de los activos en el ámbito de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.»

Tres. Se añade un apartado 3 al artículo 4, que queda redactado como sigue:

«3. Se asume como marco regulador de la seguridad interior el modelo que en cada momento se defina, de conformidad con lo establecido por el artículo 15 del Decreto 171/2020, de 13 de octubre, de conformidad con lo que establezca el Comité Corporativo de Seguridad.»

00259662

Cuatro. Se modifica el artículo 5, que queda redactado como sigue:

«Artículo 5. Objetivos, principios y definiciones.

En el ámbito de la presente orden se aplicarán las definiciones, objetivos y principios establecidos, respectivamente, en los artículos 2, 4 y 5 del Decreto 1/2011, de 11 de enero, así como las definiciones, objetivos y principios previstos, respectivamente en el en Glosario de Términos incluido como Anexo I, el artículo 4 y 5 del Decreto 171/2020, de 13 de octubre.»

Cinco. Se modifica el título del Capítulo II de la Orden que queda redactado como sigue:

«CAPÍTULO II

Política de seguridad interior y seguridad TIC»

Seis. Se modifica el artículo 6, que queda redactado como sigue:

«Artículo 6. Contexto.

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

Asimismo 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.»

Siete. Se modifica el artículo 7, que queda redactado como sigue:

«Artículo 7. Obligaciones generales.

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

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

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

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

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

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

00259662

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. Las diferentes unidades organizativas identificarán los requisitos de seguridad a incluir para la adquisición de productos.

h) Seguridad por defecto. Con anterioridad a la puesta en servicio de cualquier sistema de información será obligatorio verificar que cumple los requisitos y especificaciones de seguridad que se hubieran establecido.

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

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

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

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

m) Incidentes de seguridad.

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

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

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

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

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

00259662

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

Ocho. Se añade un artículo 11bis, que queda redactado como sigue:

«Artículo 11bis. 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.

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.»

Nueve. Se modifica el apartado 2 del artículo 12, que queda redactado como sigue:

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

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

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

00259662

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

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

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

a) En la Consejería de Transformación Económica, Industria, Conocimiento y Universidades:

1.º Comité de Seguridad Interior y Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La Unidad de Seguridad TIC.
5.º La Unidad de Seguridad Interior.
6.º La persona responsable de seguridad TIC.
7.º Las personas responsables del sistema.

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

8.º La figura del responsable del tratamiento.
9.º La figura del encargado del tratamiento.

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

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

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

Diez. Se modifica el artículo 13, que queda redactado como sigue:

«Artículo 13. Creación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

Se crea el Comité de Seguridad Interior y Seguridad TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades 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.»

Once. Se modifica el artículo 14, que queda redactado como sigue:

«Artículo 14. Composición del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades estará compuesto por los siguientes miembros:

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

00259662

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

c) Las vocalías, que serán desempeñadas por:

1.º La persona titular de cada uno de los órganos directivos centrales de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades que tengan responsabilidad sobre algún sistema de información.

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

d) La secretaría será ejercida por la persona titular de la Jefatura del Servicio de Informática, con voz y voto.

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

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.»

Doce. Se modifica el artículo 16, que queda redactado como sigue:

«Artículo 16. Funciones del Comité de Seguridad Interior y Seguridad TIC.

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

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

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

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

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

e) Nombrar a la persona responsable de seguridad TIC.

f) Nombrar a las personas responsables del sistema.

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

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

i) Informar regularmente a la persona titular de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades 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 Transformación Económica, Industria, Conocimiento y Universidades, de sus directrices y sus normas de seguridad, así como del marco normativo de seguridad TIC de la Administración de la Junta de Andalucía, a los órganos competentes para su tramitación.

k) Aprobar las normas generales de seguridad TIC, además de la normativa de segundo y tercer nivel de seguridad TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

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.

00259662

m) Realizar tareas de coordinación de los comités de seguridad interior y de seguridad TIC de las entidades instrumentales vinculadas o dependientes de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

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

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

o) Coordinar y aprobar los planes de continuidad de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

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

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

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

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

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

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

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

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

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

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

2. 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 TIC.

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.

00259662

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.»

Trece. Se modifica el apartado 1 del artículo 17, que queda redactado como sigue:

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

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

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

Catorce. Se modifica el artículo 21, que queda redactado como sigue:

«Artículo 21. Unidad de Seguridad TIC y Unidad de Seguridad Interior.

1. En virtud de lo establecido en el artículo 11.1 del Decreto 1/2011, de 11 de enero, la Consejería de Transformación Económica, Industria, Conocimiento y Universidades contará con una Unidad de Seguridad TIC, garantizando el cumplimiento del principio de función diferenciada recogido en el artículo 5.j) de dicho decreto. A estos efectos, esta Unidad estará adscrita a la Secretaría General Técnica.

La Unidad de Seguridad TIC de la Consejería de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades 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.

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

La Unidad de Seguridad Interior de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades 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

00259662

en materia de seguridad interior y la propuesta de un Plan de Seguridad Interior para la Consejería.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. El nombramiento y cese de las personas responsables y aquellas que componen las Unidades de Seguridad TIC y de Seguridad Interior de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades, 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.»

Quince. Se modifica el apartado 3 del artículo 39, que queda redactado como sigue:

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

00259662

Dieciséis. Se modifica el apartado 1 del artículo 41, que queda redactado como sigue:

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

Diecisiete. Se modifica el apartado 2 del artículo 42, que queda redactado como sigue:

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

Dieciocho. Se modifica el artículo 43, que queda redactado como sigue:

«Artículo 43. Persona delegada de protección de datos.
1. La figura de delegado de protección de datos será designada atendiendo a sus cualidades profesionales, en particular deberá tener un perfil jurídico especializado y práctica en materia de protección de datos, de conformidad con lo establecido en los artículos 37 y 38 del RGPD y los artículos 34 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre.
2. El delegado de protección de datos no recibirá ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave en su ejercicio.
3. La designación, nombramiento y cese del delegado de protección de datos deberá comunicarse en el plazo de diez días al Consejo de Transparencia y Protección de Datos de Andalucía.»

Diecinueve. Se modifica el apartado 1 del artículo 46, que queda redactado como sigue:

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

Disposición final primera. Referencias a la Consejería de Economía, Conocimiento, Empresas y Universidad.

Todas las referencias realizadas a la Consejería de Economía, Conocimiento, Empresas y Universidad que se contienen en la Orden de 12 de julio de 2019, se

00259662

entenderán realizadas a la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

Disposición final segunda. Referencias al Comité de Seguridad TIC.

Todas las referencias realizadas al Comité de Seguridad TIC que se contienen en la Orden de 12 de julio de 2019 deben entenderse realizadas al 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, 4 de abril de 2022

ROGELIO VELASCO PÉREZ
Consejero de Transformación Económica, Industria, Conocimiento y Universidades

00259662