3. Otras disposiciones

CONSEJERÍA DE JUSTICIA, ADMINISTRACIÓN LOCAL Y FUNCIÓN PÚBLICA

Orden de 7 de diciembre de 2023, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería.

De conformidad con el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Esquema Nacional de Seguridad (en adelante, ENS) tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la referida ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

La regulación del referido Esquema Nacional de Seguridad viene dada por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el cual ha derogado la normativa anterior constituida por el Real Decreto 3/2010, de 8 de enero.

Para dar cumplimiento a los requisitos y finalidades del ENS en su propio ámbito, la Junta de Andalucía aprobó el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía. Su artículo 10 ordena que cada Consejería y entidad incluida en su ámbito de aplicación disponga formalmente de su propio Documento de Política de Seguridad TIC aprobado por su persona titular. Además, establece que cada Consejería y ente instrumental de la Administración de la Junta de Andalucía deberá contar con un Comité de Seguridad TIC, que no tendrá carácter colegiado y que actuará como órgano de dirección y seguimiento en materia de seguridad de los activos TIC de su titularidad o cuya gestión tenga encomendada.

Posteriormente, se aprobó 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, el cual tiene por objeto el establecer una política de seguridad interior en la Administración de la Junta de Andalucía 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.

El artículo 9 del precitado decreto estableció que las normas de creación de los Comités de Seguridad TIC de las Consejerías modificarían su denominación, añadiendo su definición como órganos de dirección y seguimiento en materia de seguridad interior y actualizando, en caso de ser necesario, la composición y régimen de los mismos, describiendo las nuevas funciones a incorporar.

Por su parte, por la disposición adicional vigesimosegunda de la Ley 3/2020, de 28 de diciembre, del Presupuesto de la Comunidad Autónoma de Andalucía para el año 2021, se creó la Agencia Digital de Andalucía, cuyos Estatutos fueron aprobados mediante el Decreto 128/2021, de 30 de marzo. Entre los fines de esta Agencia figura la materia de la Seguridad TIC. En este sentido, el artículo 6.3, letras ñ) y u), de dichos Estatutos establece que para el ejercicio de sus fines corresponden a la Agencia, entre otras, las funciones y competencias relativas al desarrollo y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía y del sector público andaluz y al asesoramiento y asistencia técnica en tecnologías de la información y la comunicación.

El Decreto del Presidente 10/2022, de 25 de julio, sobre reestructuración de Consejerías, crea la Consejería de Justicia, Administración Local y Función Pública, estableciendo las competencias de la misma. En concreto, y tras la modificación

00293978

operada por el Decreto del Presidente 16/2022, de 3 de noviembre, le corresponden las competencias en materia de justicia, regeneración, entes instrumentales y Administración Local que actualmente tiene atribuidas la Consejería de Turismo, Regeneración, Justicia y Administración Local y las que en materia de Administración Pública venía ejerciendo la Consejería de la Presidencia, Administración Pública e Interior.

La disposición transitoria sexta del Decreto 164/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería de Justicia, Administración Local y Función Pública, señala que en tanto no se disponga de una Política de Seguridad TIC y Seguridad Interior, se seguirá aplicando las órdenes vigentes que establecen las políticas de seguridad de las tecnologías de la información y comunicaciones en el ámbito de las Consejerías que tenían asumidas las competencias en materia de justicia, administración local y función pública. Esto es, la Orden de 16 de diciembre de 2019, de la Consejería de Turismo, Regeneración, Justicia y Administración Local, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería, y la Orden de 30 de agosto de 2018, de la Consejería de la Presidencia, Administración Local y Memoria Democrática, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones así como el marco organizativo y tecnológico en el ámbito de la Consejería.

Con la presente orden se cumple con la necesidad de contar con una Política de Seguridad TIC y Seguridad Interior plenamente ajustada a la estructura actual de la Consejería.

En la elaboración de esta orden se han tenido en cuenta el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, se ha tenido en cuenta la integración transversal del principio de igualdad de género, 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.

Igualmente, para la aprobación 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, y 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.

Así, en cuanto a los principios de necesidad y eficacia, la orden desarrolla lo previsto en el apartado 1 del artículo 10 del Decreto 1/2011, de 11 de enero, con las adaptaciones derivadas del Decreto 171/2020, de 13 de octubre, teniendo el rango normativo de orden en cumplimiento de lo dispuesto en el apartado 2 del mismo artículo. Es proporcional y eficiente al desarrollar estrictamente los mandatos normativos, ya que no impone más obligaciones a la ciudadanía ni a la Administración, regulando las figuras necesarias para el cumplimiento de la finalidad perseguida y se limita a utilizar los recursos ya existentes para dar los servicios requeridos sin que suponga ningún incremento de gasto. Respecto al principio de seguridad jurídica, se han tenido en cuenta todas las normas europeas, estatales y autonómicas de aplicación. Finalmente, por lo que se refiere al principio de transparencia, al tratarse de una norma organizativa que no afecta directamente a los derechos e intereses legítimos de la ciudadanía, se ha prescindido de los trámites de consulta, audiencia e información públicas previstos en el artículo 133 de la Ley 39/2015, de 1 de octubre.

A la vista de lo anterior y en virtud de las atribuciones conferidas por los artículos 44.2 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de

00293978

Andalucía, y 26.2.a) de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, en relación con el Decreto 164/2022, de 9 de agosto,

D I S P O N G O

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

1. Esta orden tiene como objeto establecer la política de seguridad de las tecnologías de la información y comunicaciones (en adelante TIC) en el ámbito de la Consejería de Justicia, Administración Local y Función Pública, que se ha de aplicar para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione la Consejería en el ejercicio de sus competencias.

2. Esta orden constituye el documento de política de seguridad TIC de la Consejería, y es de obligado cumplimiento, de conformidad con lo dispuesto por 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.

3. La presente orden también tiene como objeto establecer la organización funcional de la seguridad interior en la Consejería, de acuerdo con lo previsto en el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

Artículo 2. Ámbito de aplicación.

1. La política de seguridad TIC regulada en esta orden será de aplicación a todos los activos y sistemas que presten servicios y traten información mediante medios electrónicos, de los que la Consejería sea titular, tenga encomendada su gestión o sean usados para el ejercicio de las competencias que le son propias en el ámbito de la Administración, así como a todo el personal que tenga acceso a dichos sistemas.

2. La política de seguridad TIC resultará de obligado cumplimiento para las entidades vinculadas o dependientes de la Consejería, de conformidad con el Decreto 1/2011, de 11 de enero, y con el Decreto 164/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería de Justicia, Administración Local y Función Pública.

3. Se excluyen de la presente política de seguridad los activos y sistemas de la Administración de Justicia afectados por el Esquema Judicial de Interoperabilidad y Seguridad (EJIS).

4. Sin perjuicio de lo anterior y de acuerdo con lo establecido por el artículo 10 del Decreto 1/2011, de 11 de enero, las entidades vinculadas o dependientes incluidas en el ámbito de aplicación de esta orden deberán disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecúen, en su caso, las directrices comunes de la Administración de la Junta de Andalucía a sus particularidades, debiendo ser aprobado por la persona titular de cada entidad.

5. Lo regulado en la presente orden en relación con la seguridad interior será de aplicación tanto a la Consejería como a sus entidades vinculadas o dependientes.

00293978

CAPÍTULO II

Objetivos, principios y marco regulador

Artículo 3. Objetivos y principios básicos.

1. Los objetivos y principios básicos de la política de seguridad TIC son los establecidos en los artículos 4 y 5 del Decreto 1/2011, de 11 de enero, con los requisitos mínimos previstos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

2. 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.

Artículo 4. Marco regulador de la seguridad interior y de la seguridad TIC.

El marco regulador de la seguridad interior está constituido por el Decreto 171/2020, de 13 de octubre, y sus posteriores normas de desarrollo, y en materia de seguridad TIC se atendrá a lo dispuesto por la disposición adicional primera del Decreto 1/2011, de 11 de enero, sin perjuicio de cualquier otra normativa aplicable a esta Consejería en virtud de su naturaleza legal y sus competencias.

CAPÍTULO III

Organización de la seguridad interior y de la seguridad TIC

Artículo 5. Estructura organizativa en la Consejería.

1. La organización para la gestión de la seguridad TIC se conforma mediante la siguiente estructura mínima:

a) Comité de Seguridad Interior y Seguridad TIC.

b) Unidad de Seguridad TIC. La persona responsable de esta unidad tendrá la condición de responsable de seguridad TIC.

c) Responsable de seguridad TIC y responsable delegado o delegada de seguridad TIC.

d) Responsable de la información y del tratamiento.

e) Responsable del servicio.

f) Responsable del sistema.

g) Delegado o delegada de protección de datos.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrán recaer sobre una misma persona o grupo de personas, unidad o departamento, siempre teniendo en cuenta que la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios y que la figura de delegado o delegada de protección de datos deberá recaer en una única persona, que no podrá coincidir y deberá ser independiente de cualquier otra figura en la estructura de seguridad.

3. La organización para la gestión de la seguridad interior se conforma mediante la siguiente estructura mínima:

a) Comité de Seguridad Interior y Seguridad TIC.

b) Unidad de Seguridad Interior.

c) Los puntos coordinadores de seguridad interior en cada provincia.

Artículo 6. Comité de Seguridad Interior y Seguridad TIC de la Consejería.

El Comité de Seguridad Interior y Seguridad TIC de la Consejería de Justicia, Administración Local y Función Pública, en adelante Comité de Seguridad Interior y Seguridad TIC de la Consejería, es el órgano para la dirección y seguimiento de la política de seguridad interior y seguridad TIC de la Consejería, correspondiendo a la persona

00293978

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

Artículo 7. Composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería.

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

a) Presidencia: La persona titular de la Viceconsejería.

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

c) Vocalías:

1.ª Las personas titulares 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.

2.ª Una persona en representación de los órganos periféricos de la Consejería, designada por la persona titular de la presidencia, a propuesta de la persona titular de la vicepresidencia entre las distintas personas responsables delegadas de seguridad TIC en dichos órganos.

3.ª La persona que ostente el perfil de responsable de seguridad TIC de la Consejería.

4.ª La persona designada como responsable de la Unidad de Seguridad Interior.

5.ª Las personas titulares de las Coordinaciones Generales de la Viceconsejería y de la Secretaría General Técnica.

6.ª La persona que ostente el perfil responsable de seguridad TIC en cada entidad vinculada o dependiente de la Consejería.

7.ª La persona que ostente el perfil responsable de seguridad interior en cada entidad vinculada o dependiente de la Consejería.

d) Secretaría: La persona titular de la jefatura del Servicio de Sistemas de Información Sectoriales de la Agencia Digital de Andalucía destacado en la Consejería, con voz y voto. La Secretaría, además de otros cometidos inherentes a sus funciones, se encargará de convocar las reuniones por orden de la persona titular de la presidencia, preparar el orden del día y elaborar el acta de las sesiones.

2. El Comité de Seguridad Interior y Seguridad TIC de la Consejería podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de alguno de sus miembros. Asimismo, podrá recabar de personal técnico especializado, propio o externo, en calidad de asesores, la información pertinente para la toma de decisiones, así como invitar a dicho personal a las reuniones con voz y sin voto.

Igualmente el Comité, cuando proceda en función de los asuntos a tratar en el orden del día de la reunión, podrá convocar a la persona que desempeñe las funciones del delegado o delegada de protección de datos de la Consejería, en calidad de asesora en materia de protección de datos.

3. Todo el personal participante deberá guardar el debido secreto respecto de los asuntos de que hayan tenido conocimiento.

4. La composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería deberá garantizar la representación equilibrada de mujeres y hombres, conforme a lo dispuesto en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

Artículo 8. Funciones del Comité de Seguridad Interior y Seguridad TIC de la Consejería.

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

a) Aprobar el desarrollo de la normativa de seguridad TIC de segundo nivel según lo previsto en el artículo 20 de la presente orden, mediante normas que amplíen y

00293978

desarrollen, sobre la base de los mínimos establecidos, las resoluciones que se aprueben por parte de la Dirección Gerencia de la Agencia Digital de Andalucía, de conformidad con el artículo 2.5 de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

b) Coordinar a alto nivel todas las actuaciones de seguridad, velando para que la definición y el desarrollo de las mismas se adecúen en todo momento a las directrices marcadas por la política de seguridad TIC, involucrando a las diferentes áreas implicadas.

c) Definir, aprobar y realizar el seguimiento de los objetivos, iniciativas y planes estratégicos en materia de seguridad TIC.

d) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y su tratamiento queden perfectamente definidos. Especialmente, para asegurar que todos y cada uno de los miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

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

f) Velar por el desarrollo, aprobación, implantación, concienciación, formación y divulgación, así como por el cumplimiento y actualización de la política de seguridad TIC en la Consejería. Para su actualización, elevará las propuestas de revisión de la política de seguridad TIC de la Consejería, o de revisión del marco regulador de seguridad TIC de la Junta de Andalucía, a los órganos competentes para su tramitación reglamentaria.

g) Nombrar a los miembros de la Unidad de Seguridad TIC de la Consejería, así como a su responsable.

h) Velar porque la seguridad TIC se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

i) Aprobar las medidas correctoras que correspondan, derivadas de las conclusiones elaboradas por la Unidad de Seguridad TIC, de las auditorías de seguridad internas o externas que se realicen.

j) Promover la formación y concienciación en materia de seguridad TIC entre el personal de la Consejería, así como la formación continua y especializada de los miembros de la Unidad de Seguridad TIC y del delegado o delegada de protección de datos.

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

l) Impulsar los preceptivos análisis de riesgos junto a la Unidad de Seguridad TIC y los perfiles responsable de la información, responsable del servicio y delegado o delegada de protección de datos. Para ello, se deberá impulsar la determinación de los niveles de seguridad de la información tratada y de los servicios prestados, usando la valoración de los impactos que tendrían los incidentes que afectaran a la seguridad TIC.

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

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

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

00293978

o) Establecer los mecanismos necesarios de coordinación con los Comités de Seguridad Interior y Seguridad TIC de las entidades vinculadas o dependientes de la Consejería.

p) 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 del delegado o delegada de protección de datos.

q) Cuantas otras le sean encomendadas.

2. En el ámbito de la seguridad interior de la Consejería, 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) Velar por la disponibilidad de los recursos para el desarrollo de los objetivos e iniciativas definidos en el Plan de Seguridad Interior de la Consejería.

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

d) Elevar las propuestas de revisión del marco normativo y organizativo interno de la Consejería en materia de seguridad interior, o de revisión del marco general en materia de seguridad interior, a los órganos competentes para su tramitación reglamentaria.

e) Determinar las condiciones y requisitos mínimos que deben contener los Planes de Seguridad Interior de las entidades vinculadas o dependientes de la Consejería, a propuesta de la Unidad de Seguridad Interior.

f) Dictar las instrucciones y recomendaciones necesarias para la constitución de los Comités de Seguridad Interior y Seguridad TIC de las entidades vinculadas o dependientes de la Consejería.

g) Nombrar a los miembros de la Unidad de Seguridad Interior, así como designar a su responsable.

h) Aprobar el modelo de relación con los Puntos Coordinadores de Seguridad Interior.

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

j) Analizar y adoptar decisiones para la prevención o para la respuesta a incidentes susceptibles de generar una crisis de seguridad en la Consejería.

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

Artículo 9. Funcionamiento y régimen jurídico del Comité de Seguridad Interior y Seguridad TIC de la Consejería.

1. El Comité de Seguridad Interior y Seguridad TIC de la Consejería se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando lo decida la presidencia, por propia iniciativa o previa solicitud de alguno de sus miembros.

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

3. De todas las sesiones celebradas se levantará un acta con los acuerdos adoptados.

Este acta tendrá carácter de información reservada dada la naturaleza de las funciones y los contenidos a tratar por el Comité.

4. El Comité se regirá por esta orden, por la normativa reguladora de la seguridad interior y de la política de seguridad TIC en la Administración de la Junta de Andalucía, así como por el resto de normativa aplicable, la reguladora del Esquema Nacional de Seguridad y de protección de datos de carácter personal.

00293978

5. 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. Así mismo, la persona titular de la secretaría del comité podrá ser sustituida en el mismo caso por una persona que ostente una plaza en el Servicio de Sistemas de Información Sectoriales de la Agencia Digital de Andalucía destacado en la Consejería, que no podrá ser miembro de la Unidad de Seguridad TIC de la Consejería.

6. Para la válida constitución del Comité, a efectos de la celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la asistencia, presencial o a distancia, de la presidencia y de la secretaría o, en su caso, de quienes le suplan, y la de la mitad, al menos, de sus miembros.

7. La presidencia del Comité ostentará voto de calidad en caso de empate en la toma de decisiones.

Artículo 10. Unidad de Seguridad TIC.

1. La Unidad de Seguridad TIC, adscrita a la Secretaría General Técnica, ejercerá las funciones de responsabilidad de seguridad TIC de la Consejería, garantizando el principio de función diferenciada previsto en el artículo 5.j) del Decreto 1/2011, de 11 de enero.

2. Las personas integrantes de la Unidad de Seguridad TIC serán nombradas por el Comité de Seguridad Interior y Seguridad TIC de la Consejería entre el personal funcionario de la Consejería o del Servicio de Sistemas de Información Sectoriales de la Agencia Digital de Andalucía destacado en la misma o perteneciente a la Subdirección de la Agencia Digital de Andalucía que ostente la competencia en ciberseguridad, a propuesta de la persona titular de la secretaría del comité.

3. La Unidad de Seguridad TIC deberá contar con una persona responsable, que será designada por el Comité de Seguridad Interior y Seguridad TIC de la Consejería entre los integrantes de la propia Unidad.

La persona responsable de la Unidad de Seguridad TIC deberá ser designada atendiendo a sus cualidades profesionales y, en particular, a su experiencia y conocimientos contrastados, tanto técnicos como de gestión, dentro del campo de la seguridad de la información, y a su capacidad para desempeñar sus funciones.

4. Las funciones de la Unidad de Seguridad TIC serán:

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

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

c) La definición, implantación y mantenimiento de los controles de carácter organizativo para la protección de los datos, aplicaciones y sistemas, así como la realización, supervisión y mantenimiento de los análisis de riesgos de la Consejería y proponer las medidas necesarias para su tratamiento.

d) La revisión de los análisis de riesgos de forma periódica, cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves, elevando el correspondiente informe al Comité de Seguridad Interior y Seguridad TIC de la Consejería.

e) El análisis de informes de auditorías, elevando al Comité de Seguridad Interior y Seguridad TIC de la Consejería las conclusiones.

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

g) 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

00293978

de la Consejería por parte de los Servicios o Departamentos responsables de la prestación de los servicios TIC. Esto incluirá la definición de los requisitos y cláusulas de seguridad de los contratos de nuevos desarrollos, que deberán estar actualizados en todo momento. Adicionalmente, antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, la Unidad de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos a las personas responsables de la información y responsables de los servicios correspondientes.

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

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

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

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

l) La gestión de la documentación de seguridad TIC.

m) Cuantas otras le sean encomendadas por la Secretaría General Técnica.

5. La Unidad de Seguridad TIC elaborará y mantendrá un inventario de servicios y sistemas en el que se indicará expresamente las personas u órganos nombrados por el comité que asuman las figuras de responsable de la información, responsable del servicio, y responsable del sistema.

Artículo 11. Unidad de Seguridad Interior.

La Consejería, de acuerdo con lo establecido en el artículo 10 del Decreto 171/2020, de 13 de octubre, contará con una Unidad de Seguridad Interior que desempeñará las funciones relacionadas en el citado artículo y que tendrá como responsable a la persona designada por el Comité de Seguridad Interior y Seguridad TIC entre el personal funcionario de la Consejería.

Artículo 12. Responsable de seguridad TIC y responsable delegado o delegada de seguridad TIC.

1. De conformidad con el artículo 11.3 del Decreto 1/2011, de 11 de enero, la persona responsable de la Unidad de Seguridad TIC de la Consejería ostentará la condición de responsable de seguridad TIC con los deberes y responsabilidades que le asigna la normativa reguladora del ENS.

2. Cada órgano directivo periférico de la Consejería deberá contar con una persona responsable delegado o delegada de seguridad TIC, designada por la persona responsable de seguridad TIC de la Consejería, de la que dependerán funcionalmente, a propuesta de la persona titular de dicho órgano.

3. En la designación a la que se refiere el apartado anterior, el responsable de seguridad TIC especificará las funciones que, entre las propias de la Unidad de Seguridad TIC, serán delegadas en las personas responsables delegadas de seguridad TIC.

Dichas funciones se ejercerán bajo la coordinación y dirección de la persona responsable de seguridad TIC de la Consejería. Entre las funciones delegadas estarán, en todo caso, las recogidas en las letras a), f) y h) del artículo 10.4.

00293978

Artículo 13. Responsable de la información y del tratamiento.

1. Será responsable de la información la persona con capacidad de decisión sobre la finalidad, contenido y uso de la información. Esta responsabilidad recaerá en la persona titular del órgano directivo central o periférico, o en su caso, órgano colegiado en cuyo ámbito de decisión se incluya la información tratada.

2. A los efectos previstos en el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el responsable de la información tendrá asimismo, respecto de los datos personales contenidos en la información incluida en su ámbito de actuación, la consideración de responsable del tratamiento.

3. Las funciones del responsable de la información serán:

a) Determinar los niveles de seguridad de la información, realizando una categorización de la información mediante la valoración del impacto de los incidentes que puedan producirse.

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

c) Aceptar los riesgos residuales de las informaciones tratadas identificados en el análisis de riesgos y realizar su seguimiento y control, en particular los resultantes del informe al que se refiere el apartado 4.h) del artículo 10, sin prejuicio de la posibilidad de delegar esta tarea.

d) Asegurarse de que los permisos correspondientes al personal que ya no tenga que acceder a la información tratada, se revoquen o deshabiliten en los sistemas relacionados.

4. Como responsable del tratamiento, además de las funciones descritas en el apartado anterior, le corresponderá adoptar la decisión sobre la creación del tratamiento, su finalidad, así como el contenido y uso de los datos tratados a lo largo de todo el ciclo de vida del tratamiento. La información actualizada de dicho responsable junto a sus tratamientos se recogerá en el Registro de Actividades de Tratamiento de la Consejería, de conformidad con lo establecido en el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre.

Artículo 14. Responsable del servicio.

1. Será responsable del servicio la persona con capacidad de decisión sobre las características del servicio a prestar. Esta responsabilidad recaerá en la persona titular del órgano directivo central o periférico, o en su caso, órgano colegiado en cuyo ámbito de decisión se incluya la determinación de las características del servicio a prestar.

2. Las funciones del responsable del servicio serán:

a) Determinar los niveles de seguridad de los servicios, realizando una categorización de los servicios mediante la valoración del impacto de los incidentes que puedan producirse.

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

c) Aceptar los riesgos residuales de los servicios prestados identificados en el análisis de riesgos y realizar su seguimiento y control, en particular los resultantes del informe al que se refiere el apartado 4.h) del artículo 10, sin prejuicio de la posibilidad de delegar esta tarea.

00293978

d) Asegurarse de que los permisos correspondientes al personal que ya no tenga que acceder al servicio prestado, se revoquen o deshabiliten en los sistemas relacionados.

Artículo 15. Responsable del sistema.

1. Será responsable del sistema la persona o personas con la responsabilidad de implantar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. La persona titular de la jefatura del Servicio de Sistemas de Información Sectoriales de la Agencia Digital de Andalucía destacado en la Consejería designará a la persona o personas responsables del sistema en caso de sistemas de información cuya implantación, operación y mantenimiento se lleve a cabo por parte de la Consejería. Para cada sistema de información deberá existir al menos un responsable del sistema, siendo posible que una misma persona sea responsable de varios o de todos los sistemas.

3. Las funciones del responsable del sistema serán:

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

b) Velar porque la seguridad TIC esté presente en todas y cada una de las partes del ciclo de vida del sistema, contemplando que las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía se sigan en el desarrollo del sistema. Además deberá verificar de forma previa a su publicación, que existen y están actualizadas las cláusulas y requisitos de seguridad particulares especificados por la Unidad de Seguridad TIC, en los posibles contratos relacionados con el sistema, y posteriormente durante el desarrollo del sistema deberá verificar su cumplimiento. Para ello podrá contar con el asesoramiento de la Unidad de Seguridad TIC.

c) Asesorar en la definición de la tipología y política de gestión del sistema, definiendo los criterios de uso y los servicios disponibles en el mismo.

d) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

e) Crear y gestionar la documentación de seguridad del sistema, con el asesoramiento de la Unidad de Seguridad TIC.

f) Asesorar, en colaboración con la Unidad de Seguridad TIC, a los responsables de la información y a los responsables de los servicios en el proceso de análisis y la gestión de riesgos.

g) Investigar los incidentes de seguridad que afecten al sistema, y en su caso, comunicarlos al responsable de seguridad TIC o a quién éste determine.

h) Suspender el tratamiento de cierta información o la prestación de un determinado servicio, previo acuerdo con la persona responsable de la Unidad de Seguridad TIC y con las personas responsables del servicio y de la información involucradas, si se detectan deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

4. En caso de sistemas de información cuya implantación, operación y mantenimiento no se lleve a cabo por parte de la Consejería, la persona titular del órgano directivo bajo cuyo ámbito se establezca la relación con el tercero encargado de dichas funciones, deberá comunicar a la Unidad de Seguridad TIC los datos de la persona responsable del sistema.

Artículo 16. Delegado o delegada de protección de datos.

1. Este perfil de responsabilidad deberá asumirse por una persona funcionaria adscrita a la Consejería atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar sus funciones de conformidad con lo establecido en los artículos 37 y 38 del Reglamento General de Protección de Datos y en los artículos 34 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre.

00293978

2. El delegado o delegada de protección de datos desempeñará las funciones previstas en la normativa en materia de protección de datos, en particular las recogidas en el artículo 39 del Reglamento General de Protección de Datos.

Artículo 17. Resolución de conflictos.

1. En caso de conflicto entre las diferentes personas u órganos responsables de la estructura organizativa en el ámbito de la seguridad TIC, este será resuelto por el Comité de Seguridad Interior y Seguridad TIC, debiendo contemplar siempre que prevalezca el mayor nivel de exigencia respecto a la seguridad.

2. En caso de conflicto entre los responsables de la estructura organizativa en el ámbito de la seguridad TIC y los responsables definidos en la normativa de protección de datos de carácter personal, este será resuelto por el Comité de Seguridad Interior y Seguridad TIC, debiendo contemplar que prevalezca la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 18. Estructura organizativa en entidades vinculadas o dependientes.

1. De acuerdo con el artículo 6.2.c) del Decreto 1/2011, de 11 de enero, y el artículo 6.1.b).1.º del Decreto 171/2020, de 13 de octubre, la organización para la gestión de la seguridad interior y de la seguridad TIC en las entidades vinculadas o dependientes de la Consejería se conforma mediante la siguiente estructura mínima:

a) Comité de Seguridad Interior y Seguridad TIC.

b) Responsable de seguridad TIC.

2. En función de las necesidades y circunstancias de la organización, las funciones de algunas de estas figuras podrá recaer sobre una misma persona, unidad o departamento, siempre teniendo en cuenta que la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

3. La responsabilidad de la conformación y designación de estas figuras en las entidades vinculadas o dependientes recaerá sobre las propias entidades.

Asimismo, de conformidad con lo previsto en el artículo 10 del Decreto 171/2020, de 13 de octubre, la entidad vinculada o dependiente contará con una Unidad de Seguridad Interior si así lo considera necesario por virtud del volumen o singularidad de sus activos. En ese caso, en la composición del Comité de Seguridad Interior y Seguridad TIC de la entidad se incluirá una persona en representación de la Unidad de Seguridad Interior.

4. Las atribuciones del Comité de Seguridad Interior y Seguridad TIC de las entidades vinculadas o dependientes podrán ser asumidas por el comité de dirección de la entidad.

5. Los nombramientos realizados para los distintos perfiles de la estructura organizativa de seguridad TIC en las entidades vinculadas o dependientes deberán comunicarse al Comité de Seguridad Interior y Seguridad TIC de la Consejería.

CAPÍTULO IV

Gestión de la seguridad TIC

Artículo 19. Directrices de seguridad.

Los principios básicos asumidos por la política de seguridad TIC de la Consejería se concretan en un conjunto de directrices particulares y responsabilidades específicas que se enmarcan en los siguientes ámbitos:

a) Tratamiento seguro de la información: Los activos TIC de información deberán inventariarse asociando a cada uno de ellos los datos de la persona responsable de los mismos y categorizarse de acuerdo a lo establecido por el ENS, en función de su sensibilidad y criticidad para el desarrollo de la actividad de la Consejería. Dicha categorización será la que determine el nivel de protección y las medidas a aplicar

00293978

sobre el activo para garantizar la confidencialidad, la integridad y la disponibilidad de la información.

b) Tratamientos de datos de carácter personal: Los tratamientos de datos de carácter personal que se efectúen en el marco de la actividad de los diferentes órganos directivos de la Consejería se ajustarán a lo dispuesto en el Reglamento General de Protección de Datos, en la Ley Orgánica 3/2018, de 5 de diciembre, y en su normativa de desarrollo. La gestión de la seguridad de los datos de carácter personal se basará en la aplicación de las medidas técnicas y organizativas apropiadas teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines de los tratamientos realizados, los riesgos para los derechos y libertades de las personas físicas y el estado de la técnica y los costes de aplicación de conformidad con el artículo 32 del Reglamento General de Protección de Datos.

c) Acceso y uso de activos TIC: Para un uso correcto, ordenado y seguro de los activos TIC puestos a disposición del personal que presta sus servicios bajo el ámbito de aplicación de esta orden, se deberá contemplar lo dispuesto por las instrucciones y normas de carácter horizontal que regulen el comportamiento del personal empleado público en el uso de los sistemas informáticos y redes de comunicaciones de la Administración de la Junta de Andalucía.

d) Seguridad física y ambiental: Los activos TIC se emplazarán en áreas seguras, protegidas mediante controles de acceso físicos acordes a su nivel de criticidad que impidan la interferencia humana, sea esta intencionada o accidental. Igualmente, se dispondrán medidas de protección contra factores externos y ambientales adversos.

e) Seguridad ligada al personal: Todas las personas que presten servicios en la Consejería tendrán la obligación de conocer y cumplir la presente política de seguridad TIC y su normativa de desarrollo. Se implantarán los mecanismos necesarios para que cualquier persona que se incorpore a la Consejería o pueda acceder a alguno de sus activos TIC sea informado del marco regulador de seguridad aplicable y conozca sus responsabilidades, reduciendo de este modo el riesgo derivado de usos indebidos. El incumplimiento manifiesto de la presente política de seguridad TIC o la normativa de seguridad derivada de ésta podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales que correspondan. Se dispondrán los medios necesarios para la articulación de iniciativas y actividades de formación y concienciación en seguridad TIC destinadas a lograr la adecuada capacitación de las personas empleadas públicas de los órganos alcanzados por esta norma. Entre tales actividades se incluirán las de difusión de esta política de seguridad TIC y de su desarrollo regulador, las dirigidas a la prevención de amenazas o aquellas relativas a la protección de datos personales. Las personas con responsabilidad en el uso, operación o administración de sistemas de información tendrán derecho a recibir formación para su uso seguro y a ser informados de sus deberes y obligaciones en materia de seguridad en la medida en que la necesiten para realizar su trabajo.

f) Control de acceso: Se limitará el acceso lógico a los activos TIC de acuerdo a su criticidad, implantando para ello mecanismos de identificación, autenticación y autorización de usuarios en relación a las funciones que estos tengan permitidas, poniendo en práctica el principio de menor privilegio o de asignación solo de los privilegios de uso necesarios para el desempeño de las tareas encomendadas. Además, cuando sea necesario, se contemplará el registro de la utilización del sistema para asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la Consejería.

g) Seguridad en la gestión de comunicaciones y operaciones: Se definirán los mecanismos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC, supervisándose su estado y reportando incidencias. La información transmitida a través de redes de comunicaciones deberá protegerse de forma adecuada, teniendo en cuenta su nivel de sensibilidad y criticidad.

00293978

h) Planificación, desarrollo y mantenimiento de sistemas de información: Los sistemas se diseñarán y configurarán de forma que la seguridad TIC se garantice por defecto y se contemple en todas las fases de su ciclo de vida, desde su planificación y diseño, pasando por las fases de desarrollo y mantenimiento y alcanzando hasta su retirada. Se contemplará la operativa que permita gestionar el conocimiento de la configuración de los sistemas así como las relaciones y conexiones entre ellos, lo que propiciará la planificación y gestión de su seguridad.

i) Gestión de incidentes de seguridad y de la continuidad: Ante incidentes de seguridad TIC, el personal deberá actuar conforme a los mecanismos apropiados para su correcta identificación, registro y resolución, habilitando un sistema de gestión que permita la mejora continua de la seguridad del sistema. En la gestión de los incidentes deberán integrarse aquellos procedimientos que establezca la Dirección Gerencia de la Agencia Digital de Andalucía o el Comité de Seguridad Interior y Seguridad TIC Corporativo de la Junta de Andalucía. Igualmente, la Consejería estará integrada en el grupo atendido por el Equipo de Respuesta a Incidentes de Seguridad Informática de la Junta de Andalucía, con el que coordinará su actuación ante incidentes. Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas y mantener la continuidad de sus procesos, de acuerdo a las necesidades de nivel de servicio.

j) Relaciones con terceros: Cuando la Consejería preste servicios a otros organismos o trate información de otros organismos, se les hará partícipes de esta política de seguridad TIC, estableciendo los mecanismos de coordinación entre las organizaciones y los procedimientos de actuación frente a incidentes de seguridad que procedan.

Cuando la Consejería utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta política de seguridad TIC y de la normativa de seguridad que aplique. Dicha tercera parte quedará sujeta, a través de cláusulas contractuales o acuerdos de nivel de servicio, a las obligaciones generales establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán mecanismos de comunicación y resolución de incidencias. Se deberá garantizar que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos, al mismo nivel que el establecido en esta política.

Cuando algún aspecto de esta política de seguridad TIC no pueda ser satisfecho por el tercero, la Unidad de Seguridad TIC emitirá un informe que precise los riesgos en que se incurre y la forma de tratarlos, requiriendo la aceptación, en su caso, de las personas responsables de la información y responsables de los servicios afectados. Los referidos responsables deberán responder al informe en un plazo no superior a treinta días, entendiéndose rechazado de no responderse en el plazo señalado.

La Consejería podrá contar con la ayuda de terceros para mejorar sus sistemas de seguridad, mediante la contratación de auditorías, asistencias técnicas o desarrollos especializados.

Artículo 20. Desarrollo normativo de la seguridad TIC.

1. Las medidas contenidas en el cuerpo normativo de seguridad TIC se desarrollarán en cuatro niveles con diferente ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento de desarrollo se fundamente en el nivel superior. Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como a la normativa aplicable en materia de protección de datos de carácter personal.

2. Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de seguridad TIC, constituido por esta orden. Será de obligado cumplimiento en toda la Consejería.

b) Segundo nivel: Normas de seguridad. Describirán de forma general los principios y ámbitos de seguridad que serán concretados en los niveles posteriores y serán de obligado cumplimiento en toda la Consejería. En general serán resoluciones de

00293978

la Dirección Gerencia de la Agencia Digital de Andalucía. Sin embargo, el Comité de Seguridad Interior y Seguridad TIC de la Consejería podrá aprobar normas propias para la Consejería, sobre la base de los mínimos establecidos, desarrollando o ampliando dichas resoluciones.

c) Tercer nivel: Procedimientos. Describirán las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Serán dependientes de las normas de seguridad.

d) Cuarto nivel: Guías técnicas. En este último nivel se podrá incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad.

3. Además de los documentos que conforman los niveles anteriores, la documentación de seguridad TIC podrá contar con las guías e instrucciones que publiquen los centros expertos para la gestión de la seguridad de ámbito estatal y autonómico así como con otros documentos de carácter no vinculante, como pueden ser recomendaciones, informes, registros o evidencias electrónicas.

4. En virtud del apartado 4 del artículo 2 de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad TIC en la Administración de la Junta de Andalucía, la Consejería desarrollará los procedimientos y guías técnicas, que tendrán el carácter de recomendaciones.

5. La Unidad de Seguridad TIC será la encargada de la gestión de la documentación de seguridad TIC.

6. El Comité de Seguridad Interior y Seguridad TIC de la Consejería establecerá los mecanismos necesarios para compartir la documentación del marco regulador con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación.

7. La siguiente tabla resume el marco de desarrollo y la responsabilidad de su aprobación dentro de la Consejería:

NIVEL	DOCUMENTO	APRUEBA
Primero	Política de seguridad	Persona titular de la Consejería
Segundo	Normas de seguridad	Comité de Seguridad Interior y Seguridad TIC de la Consejería
Tercero	Procedimientos	Persona titular de la Secretaría General Técnica
Cuarto	Guías técnicas	Persona titular de la jefatura del Servicio de Sistemas de Información Sectoriales de la Agencia Digital de Andalucía destacado en la Consejería

Artículo 21. Gestión de riesgos.

1. La Consejería asume el compromiso de controlar los riesgos de seguridad y dar cumplimiento a la normativa vigente mediante un proceso continuo de gestión de riesgos.

El establecimiento de dicho proceso seguirá las normas, guías y recomendaciones establecidas a tal efecto por el Centro Criptológico Nacional.

2. El proceso de gestión de riesgos comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas.

3. Según lo dispuesto por el Reglamento General de Protección de Datos, en el análisis de riesgos también se deberán contemplar aquellos específicos de los tratamientos de datos de carácter personal.

4. Las personas encargadas de la categorización de los sistemas serán los responsables de la información y de los servicios, siendo la Unidad de Seguridad TIC la responsable de supervisar los análisis de riesgos y proponer las medidas de seguridad necesarias para su tratamiento, pudiendo recabar para ello información y ayuda del responsable del sistema.

5. Los responsables de la información y de los servicios son los responsables de aceptar los riesgos residuales calculados en el análisis y de realizar su seguimiento y control.

00293978

6. La Unidad de Seguridad TIC revisará el análisis de riesgos con periodicidad anual o cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves, elevando el correspondiente informe al Comité de Seguridad Interior y Seguridad TIC de la Consejería.

Artículo 22. Auditorías de la seguridad.

1. Los sistemas de información serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos de la presente política, del ENS o de cualquier otra norma que así lo requiera. Con carácter extraordinario, se realizará dicha auditoría cuando existan cambios sustanciales en la información tratada y/o los servicios prestados, ocurra un incidente de seguridad grave o se reporten vulnerabilidades graves.

2. Los informes de auditoría quedarán a disposición del Comité de Seguridad Interior y Seguridad TIC de la Consejería. Estos informes serán analizados por la Unidad de Seguridad TIC que elevará al Comité de Seguridad Interior y Seguridad TIC de la Consejería las conclusiones que procedan para que éste adopte las medidas correctoras adecuadas.

Artículo 23. Cooperación con otros órganos y administraciones en materia de seguridad.

1. En atención a la mejora continua de la gestión de la seguridad TIC, se fomentará, en coordinación con la Unidad de Seguridad TIC corporativa para los agentes externos a la Junta de Andalucía, el establecimiento de mecanismos de comunicación con otros agentes especializados en esta materia, como pueden ser:

a) Agencia Digital de Andalucía.

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

c) AndalucíaCERT: Equipo de Respuesta a Incidentes de Seguridad TIC de la Junta de Andalucía.

d) CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional.

e) INCIBE: Instituto Nacional de Ciberseguridad.

f) AEPD: Agencia Española de Protección de Datos.

g) 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.

h) Asociaciones y organizaciones de expertos, especializados en Seguridad TIC o protección de datos.

2. Adicionalmente, se mantendrán contactos con otros organismos de la Junta de Andalucía para compartir experiencias y ampliar conocimientos en esta materia.

Disposición adicional primera. Deber de colaboración de órganos y unidades de la Consejería.

Todos los órganos y unidades de la Consejería prestarán su colaboración en las actuaciones de implementación de la política de seguridad interior y seguridad TIC.

Disposición adicional segunda. Ejecución y desarrollo.

Se faculta a la persona titular de la Secretaría General Técnica de la Consejería para dictar cuantas instrucciones sean necesarias y adoptar cuantas medidas técnicas sean oportunas para la ejecución y desarrollo de esta orden.

00293978

Disposición derogatoria única. Derogación de normas.

Quedan derogadas en lo que afecta al ámbito competencial de esta Consejería, la Orden de 30 de agosto de 2018, de la Consejería de la Presidencia, Administración Local y Memoria Democrática, por la que se establece la política de la seguridad de las tecnologías de la información y telecomunicaciones así como el marco organizativo y tecnológico en el ámbito de la Consejería, y la Orden de 16 de diciembre de 2019, de la Consejería de Turismo, Regeneración, Justicia y Administración Local, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería, así como cuantas disposiciones de igual o inferior rango se opongan a lo previsto en la presente orden.

Disposición final única. Entrada en vigor.

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

Sevilla, 7 de diciembre de 2023

JOSÉ ANTONIO NIETO BALLESTEROS
Consejero de Justicia, Administración Local
y Función Pública

00293978