1. Disposiciones generales

CONSEJO AUDIOVISUAL DE ANDALUCÍA

Acuerdo de 13 de septiembre de 2022, del Consejo Audiovisual de Andalucía, por el que se aprueba la política de seguridad interior y de las tecnologías de la información y telecomunicaciones así como el marco organizativo y tecnológico en el ámbito del Consejo Audiovisual de Andalucía.

El Consejo Audiovisual de Andalucía es la autoridad audiovisual independiente encargada de velar por el respeto de los derechos, libertades y valores constitucionales y estatutarios en los medios audiovisuales, tanto públicos como privados, en Andalucía, así como por el cumplimiento de la normativa vigente en materia audiovisual y de publicidad. Su composición, competencia y funcionamiento se regula en la Ley 1/2004, de 17 de diciembre, de creación del Consejo Audiovisual de Andalucía y en su Reglamento Orgánico y de Funcionamiento, aprobado por Decreto 242/2021, de 26 de octubre.

El Real Decreto 3/2010, de 8 de enero, reguló el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, establecido en el artículo 42 de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y determinó la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. De acuerdo con lo previsto en el artículo 11.1 del Esquema Nacional de Seguridad, todos los órganos superiores de las Administraciones Públicas deberían disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad aprobada por la persona titular del órgano superior correspondiente.

En cumplimiento de dicha previsión, el Pleno del Consejo Audiovisual de Andalucía aprobó el 9 de octubre de 2013 la política de seguridad de sus sistemas de información. Asumió el compromiso de controlar sus riesgos de conformidad con la legislación vigente, bajo un proceso de mejora continua.

Posteriormente, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, han configurado un escenario en el que la tramitación electrónica debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con la ciudadanía y de relación de aquellas entre sí.

La Ley 39/2015 recoge en su artículo 13, sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. La Ley 40/2015, de 1 de octubre, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

Junto a ello, el régimen de protección de datos se ha visto modificado por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

00267927

Por su parte, el Decreto 1/2011, de 11 de enero, establece la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, y el Decreto 171/2020, de 13 de octubre, establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

La modificación del marco europeo y el español referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad en las redes y sistemas de información y el marco estratégico de la ciberseguridad ha comportado la adopción del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que deroga el Real Decreto 3/2010, de 8 de enero.

Como se establece en su exposición de motivos la actualización del ENS obedece al objetivo de alinearlo con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital.

A la vista del nuevo marco regulatorio, se ha estimado conveniente adoptar un nuevo acuerdo que actualice e integre en un único documento la política de protección de datos, de seguridad interior y de las tecnologías de la información y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito del Consejo.

En su virtud, de acuerdo con el artículo 9.1 de la Ley 1/2004, de 17 de diciembre, de creación del Consejo Audiovisual de Andalucía y con el Reglamento Orgánico y de Funcionamiento del Consejo Audiovisual de Andalucía, aprobado por el Decreto 242/2021, de 26 de octubre, por el que se establece la estructura orgánica del Consejo Audiovisual de Andalucía, el Pleno, en su reunión mantenida el día 13 de septiembre de 2022,

A C U E R D A

Actualizar la política de la seguridad interior y de las tecnologías de la información y telecomunicaciones, así como el marco organizativo y tecnológico en el ámbito del Consejo que se incorpora como anexo.

Sevilla, 13 de septiembre de 2022.- El Presidente, Antonio Checa Godoy.

A N E X O

Artículo 1. Objeto.

1. El presente acuerdo tiene por objeto actualizar la política de seguridad interior y de las tecnologías de la información y comunicaciones, en adelante seguridad, en el ámbito del Consejo Audiovisual de Andalucía, en adelante el Consejo, así como establecer el marco organizativo y tecnológico de acuerdo con la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones de la Administración de la Junta de Andalucía, en el marco de la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en adelante ENS, y de la normativa en materia de protección de datos de carácter personal y sobre transparencia pública de Andalucía.

2. El presente acuerdo constituye el Documento de Política de Seguridad TIC del Consejo. Igualmente, se establece la organización funcional de la seguridad interior en el Consejo.

00267927

CAPÍTULO I

MISIÓN, OBJETIVOS Y MARCO REGULATORIO

Artículo 2. Misión y alcance.

El Consejo Audiovisual de Andalucía es la autoridad audiovisual independiente encargada de velar por el respeto de los derechos, libertades y valores constitucionales y estatutarios en los medios audiovisuales, tanto públicos como privados, en Andalucía, así como por el cumplimiento de la normativa vigente en materia audiovisual y de publicidad.

La política de seguridad se aplicará a todos los sistemas y activos que son responsabilidad del Consejo para el ejercicio de las competencias que tiene atribuidas, siempre que sean utilizados en el ámbito de la Administración de la Junta de Andalucía, por alguno de los órganos o unidades administrativas que dependan funcionalmente del Consejo. Asimismo, deberá ser observada por todo el personal del Consejo, así como por aquellas personas que tengan acceso a sus sistemas de información.

Artículo 3. Objetivos.

Son objetivos de la política de seguridad TIC y de la organización de la seguridad interior:

a) Garantizar la seguridad TIC y proteger los activos o recursos de información.

b) Crear la estructura de la organización de la seguridad TIC e interior del Consejo.

c) Marcar las directrices, los objetivos y los principios básicos de seguridad TIC del Consejo.

d) Orientar la organización para la prestación de servicios basados en la gestión de riesgos.

e) Servir de base para el desarrollo de las normas, procedimientos y procesos de gestión de la seguridad TIC.

Artículo 4. Marco regulatorio.

El marco normativo en que se desarrollan las actividades del Consejo Audiovisual de Andalucía en el ámbito de la prestación de los servicios electrónicos a los ciudadanos está compuesto por las normas aplicables a la administración electrónica, seguridad de la información y seguridad interior de la Administración de la Junta de Andalucía.

Artículo 5. Principios básicos.

La presente política de seguridad asume las definiciones, objetivos y principios establecidos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad; el Decreto 1/2011, de 11 de enero, establece la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, y el Decreto 171/2020, de 13 de octubre, establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

CAPÍTULO II

LOS ROLES Y FUNCIONES DE SEGURIDAD

Artículo 6. Organización y gestión de la seguridad. TIC y seguridad interior.

1. La estructura organizativa de la gestión de la seguridad TIC y de la gestión de la seguridad interior del Consejo está compuesta por las siguientes figuras:

a) El Comité de Seguridad Interior y Seguridad de las Tecnologías de la Información y Comunicaciones, en adelante Comité de Seguridad Interior y Seguridad TIC.

b) Responsable de Seguridad TIC.

00267927

c) Responsable de Seguridad Interior.
d) Responsable de la Información.
e) Responsable de los Sistemas.
f) Responsable de los Servicios.

2. Además, en el ámbito del Consejo, las siguientes figuras ostentan atribuciones directamente relacionadas con la seguridad TIC que son las que les asigna la normativa sobre protección de datos de carácter personal:

a) Responsable del tratamiento de datos de carácter personal.
b) Encargados de los tratamientos de datos de carácter personal.
c) El Delegado de Protección de Datos.

Artículo 7. Responsable de Seguridad TIC.

1. El Consejo, de acuerdo con lo establecido en el artículo 11 del Decreto 1/2011, de 11 de enero, contará con un Responsable de Seguridad TIC, garantizando el principio de función diferenciada recogido en el artículo 5.j) de dicho decreto, que ejerza las funciones de Responsabilidad de Seguridad TIC del Consejo, debiendo ser designada la persona responsable entre personal funcionario al servicio del Consejo por el Comité y no pudiendo ser la misma persona que el responsable establecido en el artículo 10.

2. El Responsable de Seguridad TIC determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones al comité de seguridad Interior y TIC.

Asimismo tendrá las siguientes atribuciones, de acuerdo con lo dispuesto en el art. 11.1 del Decreto 1/2011, de 11 de enero:

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

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

c) 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 del Consejo.

d) Supervisión sistemática de los controles de carácter procedimental, operacional y medidas técnicas de protección de los datos, aplicaciones y sistemas del Consejo.

e) 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 del Consejo por parte de los Servicios o Departamentos responsables de la prestación de los servicios de tecnologías de la información y comunicaciones. Antes de la puesta en producción de nuevos sistemas de información o de evolutivos de los existentes, el Responsable de Seguridad TIC deberá evaluar los aspectos de seguridad y comunicar los posibles riesgos al Responsable de la Información y Responsable del Servicio.

f) Definición y ejecución de los programas formativos y de concienciación relacionados con buenas prácticas de seguridad TIC en el ámbito del Consejo, procurando promover, en el proceso de selección de las personas participantes en estos programas, la concurrencia de mujeres.

g) Y cuantas otras le sean encomendadas por el órgano directivo del Consejo del que dependa funcional u orgánicamente.

3. Dada la existencia de relación jerárquica entre el Responsable de Seguridad TIC y el Responsable de los Sistemas, se establecerán medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del ENS.

00267927

Artículo 8. Responsable de Seguridad Interior.

1. El Consejo contará con un Responsable de Seguridad Interior que ejercerá la responsabilidad ejecutiva para la seguridad interior del conjunto de los activos en su ámbito, debiendo ser designado por el Comité de Seguridad Interior y Seguridad TIC.

2. Tendrá, en su ámbito, las siguientes funciones:

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

b) El desarrollo, el mantenimiento y la supervisión del marco regulador de la seguridad interior del Consejo.

c) La generación y supervisión de criterios y directrices para la gestión de la seguridad interior.

d) La recogida sistemática de información y la supervisión del estado de las principales variables de seguridad interior.

e) El asesoramiento técnico y la auditoría del sistema de seguridad interior en el ámbito del Consejo.

f) Definir los criterios de protección de activos especialmente sensibles a riesgos que conciernen a la seguridad interior.

g) Desarrollar planes de contingencia en respuesta a incidentes de seguridad interior, incluso situaciones de crisis.

h) Asegurar 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.

i) Promover y coordinar la cooperación con las autoridades del sector en materia de inteligencia para la seguridad.

j) Informar sobre incidentes de seguridad interior que se consideren relevantes.

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

l) Proponer al Comité de Seguridad Interior y Seguridad TIC el Plan de Seguridad Interior del Consejo, que será elevado al Pleno.

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

Artículo 9. Responsable de la información y de los servicios.

1. El responsable de la información y de los servicios será el Pleno, que desempeñará las siguientes funciones:

a) Aprobar la política de protección de datos y seguridad de la información.

b) Determinar los requisitos de la información y de los servicios prestados.

c) En el marco del Esquema Nacional de Seguridad, le corresponde la aprobación formal de los niveles y medidas de seguridad de la información y de los servicios dentro del marco de lo previsto en los anexos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Artículo 10. Responsable de los sistemas.

1. Responsable de los Sistemas será la persona adscrita a la unidad administrativa responsable de Informática designadas al efecto por la Secretaria General.

2. En el caso de sistemas de información gestionados por empresas prestatarias del servicio mediante una relación contractual, serán las personas responsables del contrato. Si el sistema de información fuera responsabilidad de otro organismo público que presta los servicios mediante convenio o disposición normativa, el responsable sería el propio responsable del sistema en el mencionado organismo. Para ambos supuestos, salvo que se designe específicamente a otra persona.

00267927

3. Sus principales responsabilidades serán:

a) Desarrollar la forma concreta de implementar la seguridad en los sistemas

b) Supervisar el desarrollo, operación y mantenimiento de los sistemas de información durante todo su ciclo de vida, así como las especificaciones de los mismos, la instalación y verificación de su correcto funcionamiento.

c) Velar porque la seguridad TIC esté presente en todas y cada una de las partes de los ciclos de vida de los sistemas de información que dirija. Especialmente porque el desarrollo de los sistemas siga las directrices de seguridad establecidas de manera horizontal por la Junta de Andalucía, de acuerdo con los criterios y requisitos técnicos de seguridad aplicables y definidos por el Responsable de Seguridad TIC del Consejo.

d) Creación, mantenimiento y actualización continua de la documentación de seguridad de los sistemas de información, con el asesoramiento del Responsable de Seguridad TIC.

e) Asesorar en la definición de la topología y sistema de gestión de los sistemas de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

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

h) Asesorar en colaboración con el Responsable de Seguridad TIC, al Responsable de la Información y los Servicios, en el proceso de la gestión de riesgos.

i) Suspender el manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser comunicada al Servicio afectado y acordada con el Responsable de Seguridad TIC, antes de ser ejecutada.

CAPÍTULO III

LA ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ PARA LA GESTIÓN Y COORDINACIÓN DE LA SEGURIDAD

Artículo 11. Creación del Comité de Seguridad Interior y Seguridad TIC.

1. Se crea el Comité de Seguridad Interior y Seguridad TIC del Consejo.

2. El Comité actuará como órgano de gestión y coordinación en materia de seguridad de los activos TIC de titularidad del Consejo o cuya gestión tenga encomendada, así como en materia de seguridad interior.

Artículo 12. Funciones del Comité de Seguridad Interior y Seguridad TIC.

1. Al Comité le corresponde aplicar, en el ámbito del Consejo, las previsiones contenidas en la normativa reguladora del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y en la normativa reguladora de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y determinar la política de seguridad que se ha de emplear en la utilización de los medios electrónicos que permita la adecuada protección de la información.

En particular, le corresponde respecto a la seguridad TIC:

a) Aprobar el desarrollo de la política de seguridad TIC de segundo nivel, según lo previsto en el artículo 15.

b) Velar por el desarrollo, implantación, concienciación, formación y divulgación, así como por el cumplimiento y actualización de la política de seguridad TIC en el Consejo.

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

00267927

d) Proporcionar, dentro de los límites establecidos en los programas asignados por las leyes anuales de presupuestos al Consejo, los medios y recursos necesarios para posibilitar la realización de las iniciativas planificadas.

e) 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.

f) Velar para que todos los ámbitos de responsabilidad y actuación en relación a la seguridad TIC y su tratamiento queden perfectamente definidos, aprobando los nombramientos necesarios para ello. Especialmente, para asegurar que la totalidad de miembros de la estructura de seguridad definida conozcan sus funciones y responsabilidades.

g) Nombrar al responsable de Seguridad TIC del Consejo.

h) Promover y fomentar la divulgación y formación en cultura de la seguridad TIC, así como la mejora continua de la seguridad en la organización, aprobando los planes de mejora de seguridad TIC propuestos por el responsable de Seguridad TIC, y velando por la asignación y cumplimiento de las responsabilidades oportunas.

i) 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.

j) Asegurar que la regulación interna que tenga incidencia en el desarrollo o explotación de sistemas de información se adecua a lo establecido en la política de seguridad TIC.

2. Al Comité le corresponde también aplicar, en el ámbito del Consejo, las previsiones contenidas en la normativa de seguridad interior.

A este respecto, le corresponde en particular:

a) Elevar al Pleno para su aprobación el Plan de Seguridad Interior propuesto por el Responsable de Seguridad Interior.

b) Realizar el seguimiento de los objetivos, iniciativas y planes definidos en el Plan de Seguridad Interior.

c) Nombrar al Responsable de Seguridad Interior.

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

e) Establecer las directrices comunes y la supervisión del cumplimento de la normativa de seguridad interior.

f) Promover la educación, el entrenamiento y la concienciación sobre medidas relativas a la seguridad interior entre el personal.

g) Llevar a cabo el análisis y la adopción de decisiones en la respuesta a incidentes susceptibles de generar una crisis de seguridad interior.

3. 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 de Protección de Datos.

Artículo 13. Composición del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC estará compuesto por las siguientes personas:

a) Presidencia: La persona titular de la Secretaria General del Consejo.

b) Vocalías: La persona titular de la Coordinación de Organización y la persona titular de Coordinación del Área Jurídica.

c) Secretaría: La persona titular del Departamento de Informática, con voz y sin voto. En los casos de vacante, ausencia, enfermedad u otra causa legal, será sustituida por una persona funcionaria adscrita a la Secretaria General.

00267927

2. En caso de vacante, ausencia, enfermedad u otras causas legales, la persona titular de la Presidencia y los vocales podrán designar una persona que les sustituya en estas circunstancias entre personal funcionario que ocupen puestos de trabajo de nivel 25 o superior.

3. En la composición del Comité ha de garantizarse, en la medida de lo posible, la representación paritaria de mujeres y hombres, conforme a lo establecido en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, y a la definición de representación equilibrada contenida en el artículo 3.3 de la Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía.

4. Los responsables de Seguridad TIC, de Seguridad Interior y el Delegado de Protección de Datos podrán asistir en calidad de asesoras a las reuniones del Comité. El Comité podrá convocar a sus reuniones a las personas que en cada caso autorice la presidencia, por propia iniciativa o a propuesta de cualquiera de sus miembros. Así mismo, podrá recabar del personal técnico especializado, propio o externo, la información pertinente para la toma de decisiones.

Artículo 14. Funcionamiento y régimen jurídico del Comité de Seguridad Interior y Seguridad TIC.

1. El Comité de Seguridad Interior y Seguridad TIC se reunirá con carácter ordinario, al menos una vez al semestre, y con carácter extraordinario, por acuerdo de la presidencia, a iniciativa propia o previa solicitud razonada de uno de sus miembros.

2. El Comité se podrá constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas, tanto de forma presencial como utilizando redes de comunicación a distancia.

CAPÍTULO IV

LAS DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO

Artículo 15. Desarrollo documental de la política de la seguridad.

1. Las medidas sobre la seguridad TIC, de obligado cumplimiento, 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.

2. Los niveles de desarrollo son los siguientes:

a) Primer nivel: Política de seguridad, constituido por el presente acuerdo. Es de obligado cumplimiento en todo el Consejo.

b) Segundo nivel: Normas de seguridad. Son de obligado cumplimiento en todo el Consejo y deben ser aprobadas por el Comité de Seguridad Interior y Seguridad TIC. Describen de forma general los principios y normas de seguridad que serán concretados en los niveles posteriores.

c) Tercer nivel: Procedimientos. Describen las acciones a realizar, de una manera más específica, en un proceso relacionado con la seguridad. Son dependientes de las normas de seguridad. Los aprueba la persona titular de la Secretaría General.

d) Cuarto nivel: Documentación técnica. En este último nivel se puede incluir todo tipo de documentación técnica o especializada que se considere necesario para completar y facilitar el desarrollo de las medidas de seguridad. Será aprobada por la persona titular del Departamento de Informática.

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

00267927

La siguiente tabla resume el marco de desarrollo y la competencia para su aprobación:

Nivel	Documento	Aprueba
Primero	Política de seguridad	El Pleno del Consejo Audiovisual de Andalucía
Segundo	Normas de seguridad	Comité de Seguridad Interior y Seguridad TIC
Tercero	Procedimientos	Persona titular de la Secretaría General
Cuarto	Documentación técnica	Persona titular del Departamento de Informática

4. El Responsable de Seguridad TIC se encarga de la gestión de los documentos indicados, debiendo asegurar que ésta sea completa y proporcione información suficiente para definir las necesidades de protección de la información y los activos asociados a la misma en el ámbito del Consejo.

5. La gestión de los riesgos para la seguridad interior se acomodará a lo previsto en el Plan de Seguridad Interior del Consejo, que será aprobado por el Pleno, tras sus elevación por Comité de Seguridad Interior y Seguridad TIC, a propuesta del Responsable de Seguridad Interior.

CAPÍTULO V

LOS RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE LOS DATOS PERSONALES

Artículo 16. Incidencia de la normativa de protección de datos personales.

1. Para el desarrollo de la política de seguridad TIC del Consejo se seguirá en todo momento lo establecido en el Reglamento General de Protección de Datos, en la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, sus normas de desarrollo y la legislación sectorial aplicable.

2. Para todos los tratamientos de datos personales del Consejo, automatizados o no, deberán establecerse las medidas técnicas y organizativas apropiadas para garantizar una seguridad adecuada de los citados datos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

3. El establecimiento de las mencionadas medidas se realizará teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines de los tratamientos de datos personales, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas. En caso de posible conflicto entre las medidas derivadas de la protección de datos personales y otras que se deriven del desarrollo de la presente política de seguridad TIC, prevalecerá el criterio que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

Artículo 17. Responsable del tratamiento.

El Pleno del Consejo será el Responsable del tratamiento de datos personales, en los términos del artículo 4.7 del Reglamento General de Protección de Datos.

Artículo 18. Delegado de Protección de Datos.

El Consejo dispondrá de un Delegado de Protección de Datos, designado por el Pleno, a los efectos de lo establecido en los artículos 37 al 39 del Reglamento General de Protección de Datos y en el Capítulo III de la LOPDGDD.

Artículo 19. Encargados del tratamiento.

1. Será encargado del tratamiento la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Responsable del tratamiento.

2. El Consejo velará para que la elección de los Encargados del tratamiento ofrezca las garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos exigidos por el Reglamento General de Protección de Datos y garantice la protección de los derechos de los interesados, conforme establece el artículo 28.1 del citado Reglamento.

00267927

3. Cuando el Encargado del tratamiento preste su servicio en régimen de concesión, encomienda de gestión, contrato o cualquier otro vínculo jurídico, las medidas de seguridad a aplicar sobre los tratamientos de datos personales se corresponderán con las establecidas por el Consejo y se ajustarán al Esquema Nacional de Seguridad.

4. El contrato o acto jurídico que vincule al Consejo y al Encargado del tratamiento deberá atender a las condiciones establecidas en el artículo 28 RGPD y demás normativa de aplicación.

CAPÍTULO VI

LOS REQUISITOS MÍNIMOS DE SEGURIDAD

Artículo 20. Respuesta a incidentes en los sistemas de la información.

La Secretaria General del Consejo asumirá la función de la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de los sistemas de información críticos.

Artículo 21. Resolución de conflictos.

Los conflictos o discrepancias entre los diferentes responsables serán resueltos por la dirección del Consejo, oído el Comité de Seguridad Interior y Seguridad TIC del Consejo. Dicho Comité podrá proponer a la dirección del Consejo el establecimiento de un procedimiento específico para la resolución de conflictos.

Artículo 22. Gestión de personal.

1. Todo el personal que preste servicios en el Consejo tiene la obligación de conocer y cumplir la política de seguridad y la normativa de seguridad derivada, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a las personas afectadas.

2. Todo el personal que se incorpore al Consejo o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado de la política de seguridad.

3. Procederá el ejercicio de las acciones pertinentes para la exigencia de las responsabilidades legales que correspondan por el incumplimiento manifiesto de la política de seguridad o de la normativa de seguridad derivada.

4. El personal del Consejo deberá cumplir además con las instrucciones y normas 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.

5. Cualquier persona que actúe bajo la autoridad del Responsable o del Encargado de un Tratamiento de datos personales en el ámbito de aplicación de este acuerdo y tenga acceso a datos personales solo tratará dichos datos siguiendo instrucciones del Responsable, salvo que se lo impida el ordenamiento jurídico comunitario, nacional o autonómico.

6. Todo el personal que preste servicios en el Consejo está comprometido con la preservación de la seguridad interior, siendo responsable de utilizar correctamente los activos y de participar, durante el desempeño ordinario de sus funciones y tareas, en la detección precoz de cuantos indicios puedan servir a la prevención de riesgos para la seguridad interior.

Artículo 23. Análisis y gestión de riesgos.

1. La gestión de riesgos deberá realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y con reevaluación periódica de los mismos.

2. La facultad para efectuar las valoraciones para determinar las categorías de seguridad, así como, en su caso, su posterior modificación, corresponderá al responsable de la información o servicios afectados. Con base en las valoraciones señaladas, la

00267927

determinación de la categoría de seguridad del sistema corresponderá al responsable de seguridad TIC.

3. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos de carácter personal, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, así como la comunicación o acceso no autorizados a dichos datos.

4. El Pleno es el responsable de aceptar los riesgos residuales calculados en el análisis sobre la información y los servicios, respectivamente, y de verificar su control.

5. El Comité de Seguridad Interior y Seguridad TIC es responsable de realizar un seguimiento de los principales riesgos residuales asumidos por el Consejo y de recomendar posibles actuaciones respecto de ello.

6. Anualmente se revisará por la persona Responsable de Seguridad TIC el proceso de gestión de riesgos en todas sus fases, elevando el correspondiente informe al Comité de Seguridad Interior y Seguridad TIC.

Artículo 24. Clasificación y control de activos.

1. Los recursos informáticos y la información del Consejo se encontrarán inventariados, con una persona responsable asociada al mismo y, en caso de ser necesario, una persona custodia de los recursos. Los inventarios se mantendrán actualizados para asegurar su validez.

2. Los activos de información estarán clasificados de acuerdo a su sensibilidad y criticidad para el desarrollo de la actividad del Consejo, en función de la cual se establecerán las medidas de seguridad exigidas para su protección.

3. En relación con la seguridad interior, la clasificación y control de activos se acomodará a lo previsto en el Plan de Seguridad Interior del Consejo.

Artículo 25. 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 del ENS.

2. Los informes de auditoría serán presentados a la persona Responsable del Sistema competente, al Delegado de Protección de Datos, si afectara a estos, y a la persona responsable de la Seguridad TIC. Estos informes serán analizados por esta última persona que presentará sus conclusiones a la persona Responsable del Sistema para que adopte las medidas correctoras adecuadas. Los resultados obtenidos determinarán las líneas de actuación a seguir y las posibles modificaciones a realizar sobre los controles y la normativa de seguridad.

3. Con el fin de optimizar la utilización de los recursos públicos y garantizar una mejor coordinación entre seguridad TIC y seguridad de protección de datos, siempre que sea posible, las auditorías de seguridad de sistemas de información y las auditorías de protección de datos o medidas análogas de verificación, evaluación y valoración de seguridad de los tratamientos se realizarán de manera conjunta.

4. La seguridad interior se auditará en el Consejo conforme a las previsiones que se contengan en el Plan de Seguridad Interior del Consejo.

Disposición transitoria única. Adecuación al Esquema Nacional de Seguridad.

La presente política dispondrá de veinticuatro meses desde la entrada en vigor del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), para alcanzar su plena adecuación al mismo, durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto podrán mantener su vigencia y los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

00267927