3. Otras disposiciones

CONSEJERÍA DE IGUALDAD, POLÍTICAS SOCIALES Y CONCILIACIÓN

Resolución de 7 de abril de 2022, del Instituto Andaluz de la Mujer, por la que se establece la política de seguridad de las Tecnologías de la Información y Comunicaciones y Seguridad Interior así como de la protección de datos de carácter personal del Instituto Andaluz de la Mujer.

El Instituto Andaluz de la Mujer (en adelante IAM) se crea por Ley 10/1989, de 29 de diciembre, como organismo autónomo de carácter administrativo dependiente de la Consejería de la Presidencia con la finalidad de promover las condiciones para que sea real y efectiva la igualdad del hombre y la mujer, posibilitando la participación de la mujer en la vida política, económica, cultural y social y superar discriminaciones de cualquier tipo. El Reglamento del IAM, aprobado por Decreto 1/1989, de 10 de enero, determina las funciones y organización del mismo, modificado por el Decreto 120/1997, de 22 de abril (BOJA núm. 49, de 26 de abril), el Decreto 452/2004, de 6 de julio (BOJA núm. 142, de 21 de julio) y el Decreto 515/2004, de 26 de octubre (BOJA núm. 212, de 29 de octubre).

En este contexto, los avances tecnológicos en los ámbitos de la informática, las telecomunicaciones y de la sociedad de la información son ya un hecho consolidado, que afecta no sólo a la sociedad sino también a los poderes públicos como responsables de generar confianza en el uso por parte de la ciudadanía de los medios tecnológicos en sus relaciones con la Administración Pública. Para conseguir esta confianza, los medios tecnológicos utilizados deben ser seguros y, para ello, se debe garantizar la confidencialidad, integridad y disponibilidad de los sistemas, de las comunicaciones y de los servicios telemáticos, permitiendo tanto a la ciudadanía, a los profesionales y a las empresas, como a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, vienen a configurar 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 los ciudadanos y de relación de aquellas entre sí.

En concreto, la Ley 39/2015, de 1 de octubre, tiene como uno de sus objetivos centrales regular las relaciones entre las Administraciones y los ciudadanos y las empresas, teniendo en cuenta el desarrollo de las tecnologías de la información y comunicación de los últimos años y cómo éste afecta a las relaciones entre estos agentes. Igualmente pretende implantar una Administración totalmente electrónica, interconectada y transparente, mejorando la agilidad de los procedimientos administrativos y reduciendo los tiempos de tramitación.

Por su parte, la Ley 40/2015, de 1 de octubre, procura dotar a nuestro sistema legal de una norma comprensiva del régimen jurídico de las Administraciones Públicas, regulando el funcionamiento interno de cada Administración y de las relaciones entre ellas. El Estatuto de Autonomía para Andalucía, en su artículo 34, reconoce el derecho a acceder y usar las nuevas tecnologías y a participar activamente en la sociedad del conocimiento, la información y la comunicación, mediante los medios y recursos que la ley establezca. Asimismo, el artículo 58.1.2.º atribuye a la Comunidad Autónoma de Andalucía competencias exclusivas sobre el régimen de las nuevas tecnologías relacionadas con la Sociedad de la Información y del Conocimiento, en el marco de la legislación del Estado.

00259488

Por otro lado, la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, señala en su artículo 7.2 que los principios que rigen las relaciones que mantenga la Administración de la Junta de Andalucía con la ciudadanía y con otras Administraciones Públicas, a través de redes abiertas de telecomunicación, son los de simplificación y agilización de trámites, libre acceso, accesibilidad universal y confidencialidad en el tratamiento de la información, y de seguridad y autenticidad en orden a la identificación de las partes y el objeto de la comunicación. Para ello, dicha ley establece que estos sistemas deben cumplir con el requisito de existencia de medidas de seguridad que eviten la interceptación y alteración de las comunicaciones, así como los accesos no autorizados. En este mismo texto legal se abunda en materia de seguridad señalándose que los medios o soportes en que se almacenen los documentos electrónicos contarán con las medidas de seguridad que garanticen la integridad, protección y conservación de los documentos almacenados, así como la identificación de las personas usuarias y el control de acceso de los mismos.

Para el desarrollo de esta Política de Seguridad de las tecnologías de la información y las comunicaciones se ha seguido lo dispuesto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS) y su modificación mediante Real Decreto 951/2015, de 23 de octubre; 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 y su modificación mediante el Decreto 70/2017, de 6 de junio; 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.

Adicionalmente, se tienen en cuenta en esta Política de Seguridad los aspectos de seguridad digital requeridos 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 y en la legislación estatal vigente en materia de protección de datos personales (en adelante, RGPD), y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales, y garantía de los derechos digitales.

Asimismo, en esta Política de Seguridad se ha tenido en cuenta la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC, así como el contexto de la Red Corporativa de Telecomunicaciones de la Administración de la Junta de Andalucía, creada por el Acuerdo del Consejo de Gobierno de 2 de junio de 1998, y de los principales sistemas de información corporativos de las entidades que forman parte de la Administración de la Junta de Andalucía.

Además, de acuerdo con 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, la presente Política incluye dentro de su estructura organizativa el Comité de Seguridad Interior y Seguridad TIC, que supone el avance en la coordinación entre la seguridad física y la ciberseguridad, favoreciendo las sinergias posibles entre ambas materias.

Esta Política de Seguridad establece el compromiso con la seguridad de los sistemas de información, define los objetivos y criterios básicos para el tratamiento de la misma, sienta los pilares del marco normativo de seguridad en el IAM y la estructura organizativa y de gestión que velará por su cumplimiento.

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

00259488

En virtud de lo expuesto, y conforme a las competencias conferidas por el artículo 9.b) del Reglamento del IAM, aprobado por Decreto 1/1989, de 10 de enero,

D I S P O N G O

Primero. Objeto.

La presente resolución tiene por objeto definir y regular la Política de Seguridad de las Tecnologías de la Seguridad y Comunicaciones y Seguridad Interior (en adelante, Política de Seguridad) del Instituto Andaluz de la Mujer (en adelante, IAM), en cumplimiento de lo establecido en 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, modificado por el Decreto 70/2017 y 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. En la Política de Seguridad se establece el marco normativo al más alto nivel para la gestión de la seguridad integral de los activos de información y comunicaciones, así como de los activos asociados a las ubicaciones físicas y el personal, con el objetivo de preservar la continuidad del funcionamiento de los servicios.

Segundo. Ámbito de aplicación.

Esta Política es de aplicación tanto a sus servicios centrales como periféricos. También será de aplicación para todo el personal que acceda a los sistemas de información como a la propia información que sea gestionada por el IAM, con independencia de cuál sea su destino, adscripción o relación con la misma.

Tercero. Objetivos, principios y definiciones.

A los efectos previstos en esta Política será de aplicación el Glosario de términos incluido como Anexo I del Decreto 1/2011, de 11 de enero, modificado por el Decreto 70/2017 de 6 de junio, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

En materia de Política de Seguridad Interior, se asumen las definiciones, los objetivos y los principios, establecidos en los artículos 3, 4 y 5, respectivamente del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

Cuarto. Contexto tecnológico y responsabilidad general.

1. El IAM depende de forma significativa de las Tecnologías de la Información y las Comunicaciones (TIC) para alcanzar sus objetivos. En consecuencia, éstas deben ser administradas con diligencia, tomando las medidas adecuadas para protegerlas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

2. La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de los órganos contemplados en el ámbito de aplicación de esta Política, siendo estas responsables del uso correcto de los activos TIC puestos a su disposición.

3. Todas las personas que presten servicios al IAM tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la presente política de seguridad, así como la normativa de seguridad que emana de la misma, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC disponer los medios necesarios para que la información llegue a los interesados.

4. Con carácter general, para el personal del IAM será aplicable el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía aprobado por Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública o la normativa de carácter horizontal vigente en cada momento.

00259488

5. Las normas de uso de los recursos TIC serán trasladadas convenientemente, en la medida en que pueda resultar necesario o recomendable, al clausulado de los contratos suscritos por el IAM.

Quinto. Marco normativo.

5.1. Marco normativo general.

- El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, determina la política de seguridad que han de aplicar las administraciones públicas en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

- El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero, establece los principios y directrices de interoperabilidad en el intercambio y conservación de la información electrónica por parte de Administraciones Públicas.

- 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. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

- 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, modificado por el Decreto 70/2017 y 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.

- Debido al carácter personal de la información tratada en el ámbito de la administración electrónica, el IAM desarrolla sus actividades de conformidad con el Reglamento (EU) 679/2016, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, que adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679.

- Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública, por la que se aprueba el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía.

5.2. Desarrollo normativo de la seguridad.

Tomando como referencia el marco normativo general, el IAM ha desarrollado la estructura normativa de la seguridad en tres niveles:

a) Primer nivel normativo: Política de Seguridad.
La Política de Seguridad constituye el instrumento normativo al más alto nivel en la estructura normativa de la seguridad del IAM.

b) Segundo nivel normativo: Normas de Seguridad.
Las Normas de Seguridad son instrumentos de nivel medio que abarcan un área determinada de la Seguridad TIC o de la Seguridad Interior, o de manera integrada. El órgano responsable de su preparación y aprobación es el Comité de Seguridad Interior y Seguridad TIC del IAM.

c) Tercer nivel normativo: Procedimientos de Seguridad.
Los Procedimientos de Seguridad son instrumentos de nivel inferior, redactados con un mayor nivel de detalle, aplicables a un ámbito específico. El órgano responsable de su aprobación es el Comité de Seguridad Interior y Seguridad TIC del IAM.

00259488

Sexto. Principios de la seguridad.

6.1. Principios básicos.

Los principios básicos que han de tenerse en cuenta en todas las decisiones que se tomen en materia de seguridad son los establecidos en el artículo 4 del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad, y los establecidos en el artículo 5 del Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía.

6.2. Principios específicos.

Para el cumplimiento de los principios básicos, recogidos en el artículo 11 del ENS, se concretan una serie de principios particulares que inspiran las actuaciones del IAM y son los siguientes:

a) Gestión organizativa integrada de la Seguridad Interior y Seguridad TIC: Este Principio recoge la estructura organizativa establecida 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, cuyo objetivo es facilitar una futura convergencia entre la seguridad física y la Ciberseguridad.

b) Cumplimiento normativo: El IAM adoptará medidas técnico-organizativas necesarias para el cumplimiento de la normativa vigente en materia de seguridad.

c) Análisis y gestión de riesgos: se empleará la metodología reconocida internacionalmente y utilizada en el resto de organismos de la Junta de Andalucía. Las medidas adoptadas mitigarán o suprimirán los riesgos, siendo justificadas y proporcionadas.

d) Gestión personal y profesionalidad: Todo el personal del IAM relacionado con la información y los sistemas, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

e) Control de acceso: El acceso a los sistemas de información y a los activos del IAM deberá ser controlado y limitado al personal, a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones: Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Las salas estarán cerradas y dispondrán de un control de llaves.

g) Adquisición de productos: el IAM adquirirá productos de seguridad de las tecnologías de la información y comunicaciones que se vayan a utilizar de forma proporcionada a la categoría de los sistemas y su nivel de seguridad.

h) Seguridad por defecto: Los sistemas y activos deben diseñarse y configurarse de forma que garanticen la seguridad por defecto, en función de su categorización.

i) Integridad y actualización de los sistemas: el IAM deberá conocer el estado de seguridad de los sistemas: especificaciones, vulnerabilidades y actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

j) Registro de actividad para la protección de datos de carácter personal: el IAM adoptará medidas técnico-organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de probabilidad y gravedad para los derechos y libertades de las personas físicas.

k) Protección de la información almacenada o de tránsito: el IAM dispondrá de procedimientos que aseguren la recuperación y conservación de los documentos electrónicos y la información en soporte no electrónico, deberá estar protegida con el mismo grado de seguridad que ésta, de conformidad con las normas de aplicación a la seguridad de los mismos.

l) Gestión de incidentes: el IAM dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información, o los activos. Estos procedimientos cubrirán los mecanismos de detección, los criterios

00259488

de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

m) Gestión de la Continuidad: Los sistemas del IAM dispondrán de medidas de respaldo y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

n) Mejora continua: El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, el IAM aplicará los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Séptimo. Estructura organizativa de la seguridad.

Para gestionar y coordinar proactivamente la seguridad del IAM, la estructura organizativa es la siguiente:

a) Comité de Seguridad Interior y de la Seguridad TIC.
b) Responsable de la Información.
c) Responsable del Servicio.
d) Responsable del Sistema.
e) Responsable de Seguridad TIC.
f) Delegado de Protección de Datos.
g) Responsable del Tratamiento.
h) Encargado del Tratamiento.

A) Comité de Seguridad Interior y de la Seguridad TIC.

1. Composición.

1. En cumplimiento de lo establecido en el artículo 10 del Decreto 1/2011, de 11 de enero por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, y por el artículo 6 del Decreto 171/2020, de 13 de octubre por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía, se crea el Comité de Seguridad Interior y de la Seguridad TIC del IAM.

2. El Comité de Seguridad Interior y de la Seguridad TIC, tiene la siguiente composición, garantizando la representación paritaria de mujeres y hombres, conforme a lo dispuesto en el artículo 19.2 de la Ley 9/2007, de 22 de octubre, de Administración de la Junta de Andalucía:

- Presidencia del Comité de Seguridad Interior y Seguridad TIC: Persona titular de la Dirección del IAM, como Responsable de la Información de acuerdo con los niveles de responsabilidad establecidos en el ENS.
- Secretaría/o del Comité: Persona Responsable de la Seguridad TIC del IAM.
- Vocales del Comité, son las personas Responsables de los Servicios y de los sistemas del IAM.
- Vocales asesores:
  • Delegado de Protección de Datos del IAM.

El Comité de Seguridad TIC no es un comité técnico, pero recabará regularmente del personal técnico propio o externo, la información pertinente para tomar decisiones.

Los vocales asesores tendrán voz, pero no voto en el Comité de Seguridad Interior y Seguridad TIC del IAM.

Cuando el tratamiento de determinadas cuestiones lo requiera, se podrá convocar a las reuniones del Comité al personal técnico especializado, a los efectos de prestar asesoramiento experto.

3. El Comité de Seguridad Interior y Seguridad TIC deberá reunirse al menos una vez al año, previa convocatoria por parte del Secretario del Comité, debiendo levantarse acta de cada una de las reuniones. También podrán celebrarse reuniones extraordinarias, si se produjeran incidentes de seguridad graves o conflictos que pudieran afectar de manera grave a los servicios prestados por el IAM.

00259488

2. Funciones.

Son funciones del Comité de Seguridad Interior y Seguridad TIC las siguientes:

a) Definir, aprobar y hacer seguimiento de los objetivos, iniciativas y planes estratégicos en materia de Seguridad Interior y Seguridad TIC.

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

c) Elevar las propuestas de revisión de la Política de Seguridad del IAM para su aprobación por parte de la Dirección del Instituto.

d) Aprobación de la normativa de Seguridad de segundo y tercer nivel.

e) Establecer directrices comunes y supervisar el cumplimiento de la normativa de Seguridad.

f) Supervisar el nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos puestos a disposición del IAM.

g) Coordinación con los Comités de Seguridad Interior y Seguridad TIC de las entidades instrumentales, vinculadas o dependientes del IAM.

h) Promover la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad entre el personal del IAM.

i) Impulsar la determinación de los niveles de seguridad, en el que se valorarán los impactos que tendrían los incidentes que afectan a la seguridad, todo ello con la participación de las personas designadas como Responsable de la Información y Responsable del Servicio, contando con la participación de la persona designada como Responsable de Seguridad TIC y las personas integradas en la Unidad de Seguridad Interior.

j) Impulsar los preceptivos análisis de riesgos, junto con las personas designadas como Responsable de la Información y de los Servicios, contando con la participación de la persona designada como Responsable de Seguridad TIC y las personas integradas en la Unidad de Seguridad Interior.

k) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes en relación con la información, servicios y activos de su competencia, obtenidos del Análisis de Riesgos.

El Comité de Seguridad Interior y Seguridad TIC aprobará, por mayoría simple de sus miembros, sus reglas de organización, funcionamiento y adopción de acuerdos.

El Comité de Seguridad Interior y Seguridad TIC contará con un esquema de suplencias en caso de que las personas titulares no puedan acudir a las reuniones del mismo.

B) Responsable de la Información.

La persona titular de la Dirección del IAM tendrá la consideración de Responsable de la Información, y asumirá las funciones establecidas para esta figura en el ENS y la Guía CCN-STIC-801, entre otras:

- Ayudar a determinar los requisitos de seguridad de la información y/o de los servicios a prestar, identificando los niveles de seguridad de la información y/o servicios mediante la valoración de impacto sobre los mismos de los incidentes que pudieran producirse.

- Proporcionar la información necesaria al Responsable 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 del Responsable del Sistema.

- En relación con los análisis de riesgos de los sistemas de información, aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

Tiene la responsabilidad de asegurar que la información que procesa y los servicios que ofrece dicho sistema cuenten con las medidas de seguridad exigidas por la legislación.

La persona designada como Responsable de la Información deberá valorar las consecuencias que puede tener un impacto negativo sobre la seguridad en el IAM,

00259488

atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

C) Responsable de Servicio.

Las personas designadas como Responsables del Servicio (titulares de unidades y departamentos) –personas que tienen la potestad de establecer los requisitos de un servicio en materia de seguridad– serán designados por el Comité de Seguridad Interior y Seguridad TIC del IAM, a propuesta de la persona titular de la Dirección del IAM, y desempeñarán las funciones establecidas en el ENS y la Guía CCN-STIC-801, dentro del marco de la presente política.

Las personas designadas como Responsables de Servicio deberán:

1. Valorar las consecuencias que puede tener un impacto negativo sobre la seguridad de los servicios en el IAM, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

2. Proporcionar la información necesaria a la persona designada como Responsable de Seguridad TIC para realizar los preceptivos análisis de riesgos, con la finalidad de establecer las salvaguardas a implantar.

3. Aceptar los riesgos residuales de las informaciones manejadas y/o servicios prestados que sean de su competencia.

D) Responsable de los Sistemas.

Las personas designadas como Responsable de los Sistemas, (persona que se encarga de la explotación de los sistemas atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad TIC) serán designadas por el Comité se Seguridad Interior y Seguridad TIC y desempeñarán las funciones establecidas en el ENS, entre otras:

1. Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

2. Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

4. Acordar la suspensión del 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 acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

E) Responsable de Seguridad TIC.

La persona Responsable de Seguridad TIC, persona con potestad para determinar los requisitos de seguridad de los servicios y la información de la entidad- será designada por el Comité de Seguridad Interior y Seguridad TIC del IAM y será jerárquicamente independiente de la persona designada como Responsable de los Sistemas. El Responsable de Seguridad TIC del IAM desarrollará las funciones descritas en el apartado 11.2 del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las TIC en la Administración de la Junta de Andalucía.

El responsable de de Seguridad TIC del IAM elaborará y mantendrá un inventario de servicios y sistemas , con indicación expresa de las personas u órganos que asumen, para cada uno de ellos, las figuras de responsable de la información, responsable del servicio, responsable del sistema y responsable de seguridad. Dicho listado se entregará, actualizado al Comité de Seguridad Interior y Seguridad TIC del organismo en cada una

00259488

de sus reuniones, con indicación de aquellas deficiencias o faltas de información que se produzcan, de modo que el Comité disponga de información completa y pueda arbitrar los mecanismos necesarios para la subsanación de las deficiencias o faltas de información.

Octavo. Estructura organizativa en materia de Protección de Datos de Carácter Personal.

Las responsabilidades del IAM en materia de Protección de Datos son las siguientes:

Responsable del Tratamiento. Las funciones del Responsable del Tratamiento son asumidas por la persona titular de la Dirección del IAM.

Delegado/a de Protección de Datos. Las funciones del Delegado/a de Protección de Datos son las establecidas en el artículo 39 del RGPD. El/La Delegado/a de Protección de Datos velará por la elaboración y mantenimiento de un Registro de Actividades de Tratamiento de Datos de Carácter Personal en los términos del artículo 30 del RGPD.

Encargado/a del Tratamiento. Se trata de los organismos o entidades que traten datos de carácter personal por cuenta del IAM.

Noveno. Resolución de conflictos.

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

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

Décimo. Gestión de los riesgos.

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

2. Las personas Responsables de la Información, de los servicios y de los tratamientos de Datos de Carácter Personal, en su caso, son responsables de los riesgos sobre los mismos y, por tanto, de aceptar los riesgos residuales calculados en el análisis de riesgos, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

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

4. La selección de las medidas de seguridad a aplicar será propuesta por la persona designada como Responsable de Seguridad TIC, así como el seguimiento de su aplicación. Dichas medidas, en el ámbito de la Seguridad TIC serán las mínimas determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos que cumpla los requisitos del ENS. Asimismo, en el ámbito de Seguridad Interior, se estará a las medidas, en su caso, establecidas por 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, así como sus posteriores versiones, y de la normativa en materia de protección de datos de carácter personal.

5. El proceso de gestión de riesgos comprende las fases de identificación y valoración de informaciones y servicios esenciales prestados, categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, las cuales deberán ser proporcionales a los riesgos y estar justificadas. Este análisis deberá revisarse cada año por parte de la persona designada como Responsable de Seguridad TIC, que elevará el correspondiente informe al Comité de Seguridad Interior y Seguridad TIC.

00259488

6. Para realizar el análisis de riesgos TIC se utilizará la metodología MAGERIT, aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, como PILAR, desarrollada por el Centro Criptológico Nacional. El análisis de riesgos relativo a la Seguridad Interior se desarrollará conforme a la metodología empleada por la Junta de Andalucía.

Undécimo. Gestión de los incidentes de seguridad y de la continuidad.

El IAM debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS, y de lo dispuesto en su caso, por la normativa vigente en cada momento.

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

A los efectos de una mejor gestión de los incidentes TIC, se actuará de forma coordinada con Andalucía CERT.

Duodécimo. Terceras partes.

Cuando una organización, entidad, o usuario externo, tenga acceso en virtud de norma, contrato o convenio, a los sistemas de información del IAM, éste le hará partícipe de esta Política de Seguridad. En concreto, esta tercera parte quedará sujeta a través de cláusulas contractuales o acuerdos de nivel de servicio, en los que se recoja el contenido establecido en la presente Política y el cuerpo normativo en materia de Seguridad del IAM.

Se establecerán mecanismos de comunicación y resolución de incidencias. Se velará por que el personal de terceros esté adecuadamente concienciado y formado en materia de Seguridad.

Si algún aspecto de esta Política de Seguridad no puede ser satisfecho por una tercera parte según lo anterior, se requerirá un informe del Responsable de Seguridad TIC que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y/o los servicios afectados antes de proseguir en la relación con terceros.

Decimotercero. Formación y concienciación.

El IAM desarrollará con carácter anual un Plan de Formación y Concienciación en materia de Seguridad TIC y Seguridad Interior, con el objetivo de interiorizar una cultura de la seguridad alineada con la presente Política de Seguridad.

El Plan de Concienciación irá destinado al personal en general del IAM, y será desarrollado con el objetivo de dar a conocer esta Política y su desarrollo normativo.

Decimocuarto. Auditorías de seguridad.

El IAM manifiesta el compromiso de auditar los sistemas de información de forma periódica con objeto de revisar el cumplimiento normativo.

Al menos cada dos años se debería realizar una Auditoría de Seguridad, que confirme el cumplimiento de los requisitos del RGPD y su normativa de desarrollo, el ENS y 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.

Estas auditorías serán elevadas al Comité de Seguridad Interior y Seguridad TIC para que determine las líneas de actuación a seguir y las modificaciones necesarias para conducir la gestión de la seguridad del IAM a la mejora continua.

00259488

Decimoquinto. Cooperación con otros Órganos y otras Administraciones en materia de seguridad.

A efectos de coordinación, obtención de asesoramiento e intercambio de experiencias para la mejora continua de la gestión de la Seguridad, se fomentará el establecimiento de mecanismos de comunicación del IAM con otros agentes especializados en esta materia. En especial, se contemplarán los siguientes:

- Comité de Seguridad TIC de la Junta de Andalucía.
- Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.
- Comité Corporativo de Seguridad Interior de la Junta de Andalucía.
- Unidad Corporativa de Seguridad Interior de la Junta de Andalucía.
- Consejo de Transparencia y Protección de Datos de Andalucía.
- CCN-CERT: Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), como soporte y coordinación para la resolución de incidentes que sufra la Administración General, Autonómica o Local.
- Agencia Española de Protección de Datos (AEPD).
- Instituto Nacional de Ciberseguridad (INCIBE).
- Grupo de Delitos Informáticos y Telemáticos de la Guardia Civil y Brigada de Investigación Tecnológica (BIT) del Cuerpo Nacional de Policía, para la investigación de acciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones.

Decimosexto. Revisión de esta Política de Seguridad.

La presente política de seguridad debe reflejar fielmente el compromiso del IAM con la Seguridad. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad Interior y Seguridad TIC para adaptarse a cambios en el entorno legislativo, técnico u organizativo.

Decimoséptimo. Difusión de la Política de Seguridad.

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

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

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

Disposición final. Entrada en vigor.

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

Sevilla, 7 de abril de 2022.- La Directora, Laura Fernández Rubio.

00259488