3. Otras disposiciones

CONSEJERÍA DE IGUALDAD, POLÍTICAS SOCIALES Y CONCILIACIÓN

Resolución de 27 de abril de 2021, de la Agencia Andaluza de Cooperación Internacional para el Desarrollo, por la que se establece la política de seguridad de las Tecnologías de la Información y Comunicaciones y de la protección de datos de carácter personal de la Agencia Andaluza de Cooperación Internacional para el Desarrollo.

La Agencia Andaluza de Cooperación Internacional para el Desarrollo, en adelante la AACID, desde su creación por la Ley 2/2006, de 16 de mayo, tiene como objetivo optimizar, en términos de eficacia y economía, la gestión de los recursos públicos que la Administración de la Junta de Andalucía destina a la cooperación internacional para el desarrollo, contribuyendo al cumplimiento de los objetivos específicos que aquella debe perseguir con su actuación en esta materia.

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 este 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.

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

00191668

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 la Política de seguridad de las tecnologías de la información y las comunicaciones de la AACID 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.

En la elaboración de esta política de seguridad, asimismo, 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.

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 la AACID 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. 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, se integra la nueva solución organizativa consistente en la creación de un Comité de Seguridad Interior y Seguridad TIC, suponiendo un avance en la coordinación entre la seguridad física y la ciberseguridad, favoreciendo las sinergias posibles entre ambas materias.

En su virtud de lo expuesto, y conforme a las competencias conferidas por el artículo 16.1.j) de los Estatutos de la Agencia Andaluza de Cooperación Internacional para el Desarrollo, aprobados por Decreto 184/2014, de 30 de diciembre,

00191668

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 Información y Comunicaciones (en adelante, Política de Seguridad TIC) de la Agencia Andaluza de Cooperación Internacional para el Desarrollo (en adelante, AACID), en cumplimiento de los 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, que se ha de aplicar al tratamiento de la información, así como a los activos de tecnologías de la información y comunicaciones titularidad de la AACID, o cuya gestión tenga encomendada.

Segundo. Ámbito de aplicación.

Esta Política de Seguridad TIC es de aplicación a:

a) Las unidades, departamentos y áreas de la AACID, en todos sus sistemas de información y personal destinado en estas.

b) Al personal de otras entidades que, en virtud de una norma jurídica, contrato, convenio u otra figura jurídica aplicable, realicen tratamientos de información por cuenta de la AACID o tengan acceso a sus sistemas de información.

Tercero. Definiciones.

A los efectos previstos en esta Política de Seguridad TIC será de aplicación el Glosario de términos incluido como Anexo I 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.

Cuarto. Contexto tecnológico y responsabilidad general.

1. La AACID depende de forma significativa de las Tecnologías de la Información y las Comunicaciones (TIC) para alcanzar sus objetivos. En consecuencia, estas 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 a la AACID tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación, la presente Política de Seguridad TIC, así como la normativa de seguridad que emana de la misma, siendo responsabilidad del Comité de Seguridad Interior y Seguridad TIC de la AACID disponer los medios necesarios para que la información llegue a las personas que tienen la obligación de conocer y cumplir, en sus respectivos ámbitos de actuación interesados.

4. Con carácter general, para el personal de AACID 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.

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 la AACID.

00191668

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 se 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 gestiones 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.

Las Leyes 39/2015 y 40/2015, regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones. 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 a que la información tratada en el ámbito de la administración electrónica contiene datos de carácter personal la AACID 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.

5.2. Desarrollo Normativo de la Seguridad TIC.

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

a) Primer nivel normativo: Política de Seguridad TIC.

La Política de Seguridad TIC constituye el instrumento normativo al más alto nivel en la estructura normativa de la seguridad TIC de la AACID. Deberá ser aprobada por la persona titular de la Dirección de la Agencia.

b) Segundo nivel normativo: Normas de Seguridad de la Información.

Las Normas de Seguridad TIC son instrumentos de nivel medio que abarcan un área determinada de la seguridad TIC. El órgano responsable de su preparación y aprobación es el Comité de Seguridad Interior y Seguridad TIC de la AACID.

c) Tercer nivel normativo: Procedimientos de Seguridad TIC.

Los Procedimientos de Seguridad TIC son instrumentos de nivel inferior, redactados con un mayor nivel de detalle, aplicables a un ámbito específico o sistema determinado. El órgano responsable de su aprobación es el Comité de Seguridad Interior y Seguridad TIC de la AACID.

Sexto. Principios de la seguridad TIC.

6.1. Principios básicos.

Los Principios básicos que han de tenerse en cuenta en todas las decisiones que se tomen en materia de seguridad TIC son los establecidos en el artículo 4 del Real Decreto 3/2010, por el que se regula el Esquema Nacional de Seguridad.

00191668

6.2. Principios específicos.

Para el cumplimiento de los principios básicos, se concretan una serie de principios particulares que inspiran las actuaciones de la AACID. Son los siguientes:

a) Protección de datos de carácter personal: la AACID 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.

b) Seguridad ligada a las personas: Todo el personal de la AACIC 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.

c) Control de acceso: El acceso a los sistemas de información de la AACID deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

d) Gestión de incidentes: La AACID dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios 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.

e) Gestión de la Continuidad: Los sistemas de la AACID dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

f) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto.

g) Cumplimiento normativo: La AACID adoptará medidas técnico-organizativas necesarias para el cumplimiento de la normativa vigente en materia de seguridad de la información.

h) Gestión organizativa integrada de la Seguridad Interior y Seguridad TIC: Este Principio recoge la nueva 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.

Séptimo. Estructura organizativa de la Seguridad TIC.

Para gestionar y coordinar proactivamente la seguridad TIC la estructura organizativa de la seguridad TIC en la AACID es la siguiente:

a) Comité de Seguridad Interior y de la Seguridad TIC.
b) Persona Responsable de la Información.
c) Persona Responsable del Servicio.
d) Persona Responsable de Sistemas.
e) Persona Responsable de Seguridad.

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

a.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 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 TIC de la AACID.
2. El Comité de Seguridad Interior y Seguridad TIC, tiene la siguiente composición, garantizando la representación paritaria de mujeres y hombres, conforme

00191668

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 de la AACID, como Responsable de la Información de acuerdo con los niveles de responsabilidad establecidos en el ENS.
- Vicepresidencia del Comité: Persona titular de la subdirección de la AACID.
- Vocales del Comité, son las personas Responsables de los Servicios de acuerdo con los niveles de responsabilidad establecidos en el ENS:
  - Persona titular de la Jefatura de la Unidad Técnica de la AACID.
  - Persona titular de la Jefatura de la Unidad de Cooperación con Mediterráneo y Territorios Palestinos de la AACID.
  - Persona titular de la Jefatura de Unidad de Planificación y Evaluación de la AACID.
  - Persona designada como Responsable Seguridad TIC de la AACID.
  - Persona titular de la Jefatura del Departamento de Calidad y Recursos Humanos de la AACID.
- Secretaría: Persona titular del Departamento TIC de la AACID.

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 la AACID.

a.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 seguridad Interior y Seguridad TIC.
b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos y proponer a la Unidad de Seguridad TIC de la Consejería competente en materia de igualdad, políticas sociales y conciliación, la realización de los procedimientos de compra centralizada de productos y servicios corporativos de seguridad TIC, en aquellos supuestos en que se determine su conveniencia en razón a criterios de oportunidad, eficacia y de economías de escala.
c) Elevar las propuestas de revisión de la Política de Seguridad TIC de la AACID para su aprobación por parte de la persona que ostenta la Dirección de la Agencia.
d) Aprobación de la normativa de Seguridad TIC de segundo y tercer nivel.
e) Establecer directrices comunes y supervisar el cumplimiento de la normativa de seguridad TIC.
f) Supervisar del nivel de riesgo y toma de decisiones en la respuesta a incidentes de seguridad TIC que afecten a los activos TIC puestos a disposición de la AACID.
g) Promover la educación, entrenamiento y concienciación sobre las medidas legales y organizativas relativas a la Seguridad TIC entre el personal de la Administración Pública.
h) Impulsar la determinación de los niveles de seguridad de la información tratada, en el que se valorarán los impactos que tendrían los incidentes que afectarán a la seguridad de la información, todo ello con la participación de las

00191668

personas designadas respectivamente como Responsable de la Información, Responsable del Servicio y el Responsable de Seguridad TIC.

i) Impulsar los preceptivos análisis de riesgos, junto con las personas designadas como Responsable de la Información y de los Servicios que correspondan, contando con la participación de persona designada como Responsable de Seguridad TIC.

j) Coordinar la aceptación de los riesgos residuales por sus responsables correspondientes en relación con la información y servicios 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.

b) Responsable de la información.

La persona titular de la Dirección de la AACID 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. 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 de la información en AACID, 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) Responsables 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 de la AACID, a propuesta de persona titular de la Dirección de la AACID, y desempeñará las funciones establecidas en el ENS y la Guía CCN-STIC-801, dentro del marco de la presente Política. Esta designación será revisada cada dos años, o cuando el puesto quede vacante.

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 AACID, 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.

La persona titular de la Dirección de la AACID, a propuesta del titular del área o departamento correspondiente, designará a la persona Responsable del Sistema, –persona que se encarga de la explotación los sistemas atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad– que desempeñarán las funciones establecidas en el ENS. Esta designación será revisada cada dos años, o cuando el puesto quede vacante.

e) Responsable de Seguridad.

La persona designada como Responsable de Seguridad, -persona con potestad para determinar los requisitos de seguridad de los servicios y la información de la entidad- será designado por el Comité de Seguridad Interior y Seguridad TIC de la AACID y será

00191668

jerárquicamente independiente de la persona designada como Responsable del Sistema. El Responsable de Seguridad TIC de la AACID 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. Esta designación será revisada cada dos años, o cuando el puesto quede vacante.

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

Las responsabilidades de la AACID en materia de Protección de Datos son las siguientes:

a) Responsable del Tratamiento.

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

b) Delegado de Protección de Datos.

La persona titular de la Dirección de la AACID nombrará al Delegado de Protección de Datos que asumirá las funciones establecidas en el artículo 39 del RGPD.

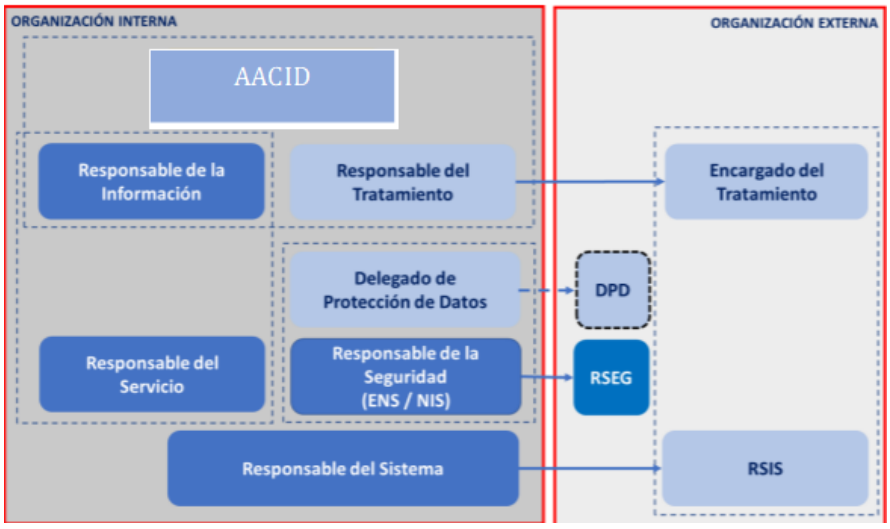
A su vez, la persona designada como Delegado de Protección de Datos velará por la elaboración y mantenimiento de un Registro de Actividades de Tratamiento de Datos de Carácter Personal en los términos del artículo 30 del RGPD.

c) Encargado del Tratamiento.

Se trata de los organismos o entidades que traten datos de carácter personal por cuenta de la AACID.

d) Esquema conceptual organizativo ENS-RGPD.

De acuerdo con la Guía CCN-STIC 801, el esquema conceptual de la estructura de la Seguridad de la Información y Protección de Datos de Carácter Personal podría representarse a través del siguiente esquema.



Se diferencia tres bloques de responsabilidad:

- Responsabilidad legal y la especificación de requisitos: que corresponde a la persona titular de la Dirección de la Agencia, y respectivamente a las personas designadas como Responsable de la Información y el Responsable del Servicio.
- La supervisión: que corresponde respectivamente a las personas designadas como Responsable de Seguridad y Delegado de Protección de Datos.
- La operación del sistema de información que corresponde a la persona designada como Responsable del Sistema.

00191668

Décimo. Gestión de los riesgos.

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y re-evaluación 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 el Responsable de Seguridad TIC, así como el seguimiento de su aplicación. Dichas medidas 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 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.

6. Para realizar el análisis de riesgos 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.

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

La AACID estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, según los términos previstos en el artículo 7 del ENS.

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

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

00191668

Decimosegundo. Terceras partes.

Cuando una organización, entidad, o usuario externo, tenga acceso en virtud de norma, contrato o convenio, a los sistemas de información de AACID, ésta le hará partícipe de esta Política de Seguridad TIC. 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 TIC de la AACID. La AACID deberá cerciorarse que el personal de terceros esté adecuadamente concienciado y formado en materia de seguridad TIC.

Decimotercero. Formación y concienciación.

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

El Plan de Formación irá destinado a las personas con responsabilidad en la operación o administración de sistemas y será desarrollado con el objetivo de adquirir destrezas en el manejo seguro de los sistemas de información.

El Plan de Concienciación irá destinado al personal en general de la AACID, y será desarrollado con el objetivo de dar a conocer esta Política de Seguridad TIC y 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.

Decimocuarto. Auditorías de seguridad.

Al menos cada dos años se realizará una auditoría de seguridad, que confirme el cumplimiento de los requisitos del RGPD y su normativa de desarrollo y el ENS.

Estas auditorías serán elevadas respectivamente a las personas designadas como Responsable de la Información y del Sistema, Responsable de Seguridad TIC y Delegado de Protección de Datos.

Los resultados obtenidos determinarán las líneas de actuación a seguir y las modificaciones necesarias para conducir la gestión de la seguridad de la AACID a la mejora continua.

Decimoquinto. 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 TIC 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.

Decimosexto. Cooperación con otros órganos y otras administraciones en materia de seguridad.

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

- Comité de Seguridad Interior y Seguridad TIC de la Consejería de Igualdad, Políticas Sociales y Conciliación.
- Comité de Seguridad TIC de la Junta de Andalucía.
- Unidad de Seguridad TIC Corporativa de la Junta de Andalucía

00191668

- 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.

Decimoséptimo. Revisión de esta política de seguridad.

La presente política de seguridad ha de ser un documento que refleje fielmente el compromiso de la AACID con la seguridad de la información. 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.

Decimoctavo. Difusión de la política de seguridad TIC.

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

Disposición adicional única. Constitución del Comité de Seguridad TIC.

La primera reunión del Comité de Seguridad TIC tras la entrada en vigor de la presente política de seguridad TIC tendrá por objeto la constitución, renovación o confirmación del mismo y se celebrará en un plazo máximo de un mes a partir de la entrada en vigor de la presente resolución.

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, 27 de abril de 2021.- La Directora, María Luz Ortega Carpio.

00191668