Política de Seguridad

Contenido

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN 3
3. ALCANCE 4
   3.1. Alcance Subjetivo 4
   3.2. Alcance Objetivo 4
4. MARCO NORMATIVO 4
5. REQUISITOS MÍNIMOS DE SEGURIDAD 5
6. PRINCIPIOS BÁSICOS 6
7. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN 7
8. MISIÓN 7
9. CUMPLIMIENTO DE ARTÍCULOS 8
10. DESARROLLO DE LA POLÍTICA 8
   10.1. Primer nivel normativo: Política de Seguridad. 8
   10.2. Segundo nivel normativo: Normas de Seguridad. 9
   10.3. Tercer nivel normativo: Procedimientos de Seguridad. 9
11. ORGANIZACIÓN DE LA SEGURIDAD 9
   11.1. Roles o perfiles de seguridad 9
   11.2. Comité de Seguridad Interior y Seguridad TIC de la AACID 9
   11.3. Responsabilidades asociadas al Esquema Nacional de Seguridad 10
   11.4. Procedimientos de designación 14
12. RESOLUCIÓN DE CONFLICTOS 14
13. DATOS DE CARÁCTER PERSONAL 14
14. TERCERAS PARTES 15
15. MEJORA CONTINUA 16

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto presentado el día 27 de noviembre de 2023 por el Comité de Seguridad Interior y Seguridad TIC de la Agencia Andaluza de Cooperación Internacional para el Desarrollo y revisado en sesión de dicho Comité celebrada el 20 de mayo de 2024.

Esta "Política de Seguridad", en adelante Política, será efectiva desde su fecha de aprobación, el 7 de febrero de 2025, tras haber sido aprobada por los miembros del Comité mediante procedimiento escrito, y se mantendrá vigente hasta que sea sustituida por una nueva Política, debiendo ser comunicada para el conocimiento general de todos los empleados y empleadas de la entidad, lo que facilitará su cumplimiento y seguimiento.

2. INTRODUCCIÓN

La Agencia Andaluza de Cooperación Internacional para el Desarrollo (en adelante, AACID) depende en gran medida de los sistemas TIC (Tecnologías de la Información y Comunicaciones) para alcanzar sus objetivos y es consciente que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan servicios públicos, y que como proveedor del sector público debe gestionar de manera adecuada estos riesgos.

El objetivo de esta gestión de riesgos es proteger los sistemas de Tecnologías de la Información y las Comunicaciones frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada por la AACID.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos de la AACID deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación

deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

3. ALCANCE

3.1. Alcance Subjetivo

Los sujetos obligados por esta Política son todo el personal de la AACID, y todas aquellas personas o entidades, sean internos o externos, que presten servicios a la AACID, tanto en sus propias instalaciones como en remoto.

3.2. Alcance Objetivo

Esta Política se aplicará a los sistemas de información[1] de la AACID relacionados con la gestión de las subvenciones convocadas por la AACID (Agenda de Tramitación).

4. MARCO NORMATIVO

El marco normativo en el que se desarrollan los servicios integrados en el alcance del ENS de la AACID, de manera no limitativa está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 (Reglamento general de protección de datos, RGPD).
- Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero.

1Los sistemas de información han de entenderse en un sentido amplio como, “aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar la información”.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

- 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 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 actualización y seguimiento del marco normativo será responsabilidad del Responsable de Seguridad y se mantendrá en el "Registro de Legislación Aplicable", incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio para la Transformación Digital y de la Función Pública.

Así mismo, la persona designada como Responsable de Seguridad de la AACID también será responsable de identificar las guías de seguridad del CCN, que serán de aplicación para mejorar el cumplimiento de lo establecido en el ENS.

5. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política de Seguridad de la AACID regula la gestión continua del proceso de seguridad. Esta Política se ha establecido de acuerdo con los principios básicos establecidos en el Capítulo II del ENS y se desarrolla teniendo en cuenta la aplicación de los siguientes requisitos mínimos de seguridad:

a) Organización e implantación del proceso de seguridad

b) Análisis y gestión de los riesgos

c) Gestión de personal

d) Profesionalidad

e) Autorización y control de los accesos

f) Protección de las instalaciones

g) Adquisición de productos de seguridad y contratación de servicios de seguridad

h) Mínimo privilegio

i) Integridad y actualización del sistema

j) Protección de la información almacenada y en tránsito

k) Prevención ante otros sistemas de información interconectados

l) Registro de la actividad y detección de código dañino

m) Incidentes de seguridad

n) Continuidad de la actividad

ñ) Mejora continua del proceso de seguridad

Para dar cumplimiento a estos requisitos mínimos la AACID aplicará las medidas de seguridad en el Anexo II del ENS teniendo en cuenta:

- Los activos que constituyen los sistemas de información de la AACID.
- La categoría de seguridad del sistema, según lo previsto en el artículo 40 del Real Decreto 311/2022, de 3 de mayo.
- Las decisiones que se adopten para gestionar los riesgos identificados.

6. PRINCIPIOS BÁSICOS

La Política de Seguridad de la AACID establece los siguientes principios básicos que han de tenerse presentes en el uso de los sistemas de información:

- Seguridad como proceso integral: la seguridad es un proceso que comprende todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información.

- Gestión integral basada en riesgos: el análisis y gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos aceptables.

- Prevención, detección, respuesta y conservación: la seguridad del sistema de información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta.

- Existencia de líneas de defensa: el sistema de información de la AACID debe disponer de una estrategia de protección constituida por múltiples capas de seguridad.

- Vigilancia continua y reevaluación periódica: la vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La

evaluación permanente permitirá medir su evolución y las medidas de seguridad se reevaluarán y actualizarán periódicamente adecuando su eficacia a la evolución de los riesgos y sistemas de protección.

7. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La AACID establece como objetivos de Seguridad los siguientes:

- Garantizar la protección de la información.
- Seguridad física: la AACID emplaza los sistemas de información en áreas seguras, protegidas por controles de acceso físico adecuados a su nivel de criticidad.
- Control de acceso: la AACID limita el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de mecanismos de identificación, autenticación y autorización adaptados a la criticidad de cada activo.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: la AACID contempla los aspectos de seguridad en todas las fases del ciclo de vida de los sistemas de información.
- Garantizar la prestación continuada de los servicios: la AACID implanta los procedimientos adecuados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de los procesos de negocio.
- Protección de datos: la AACID adopta las medidas técnicas y organizativas necesarias para gestionar los riesgos derivados del tratamiento de datos personales.
- Cumplimiento: la AACID adopta las medidas técnicas y organizativas necesarias para el cumplimiento de la normativa legal vigente en materia de Seguridad de la Información.

8. MISIÓN

De acuerdo con la previsión contenida en el Estatuto de Autonomía para Andalucía, y en desarrollo de la planificación prevista en la Ley 14/2003, de 22 de diciembre, de Cooperación Internacional para el Desarrollo), el objetivo de la AACID, según la Ley 2/2006, de 16 de mayo, por la que se crea, es 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 específicos objetivos que aquélla debe perseguir con su actuación en esta materia.

9. CUMPLIMIENTO DE ARTÍCULOS

Para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, la AACID ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y servicios a proteger teniendo en cuenta la categoría de los sistemas afectados.

10. DESARROLLO DE LA POLÍTICA

El Comité de Seguridad Interior y Seguridad TIC de la AACID ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad Interior y Seguridad TIC la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte de la Dirección de la AACID.

La presente Política de Seguridad es de obligado cumplimiento y se estructura a nivel documental, en los siguientes niveles jerárquicos:

- Primer nivel: Política de Seguridad.
- Segundo nivel: Normativas de Seguridad.
- Tercer nivel: Procedimientos de Seguridad.

El Responsable de Seguridad deberá revisar al menos con periodicidad anual esta normativa, proponiendo mejoras a la misma en el caso que sea necesario.

El personal de la AACID y terceras empresas, deberán conocer además de esta Política de Seguridad, todas las normativas, procedimientos, instrucciones técnicas, u otra documentación que pueda afectar en el desempeño de sus funciones.

10.1. 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 de la AACID. Deberá ser aprobada por la Dirección de la AACID.

10.2. Segundo nivel normativo: Normas de Seguridad.

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

10.3. 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, y serán aprobados por el Responsable de Seguridad de la AACID.

11. ORGANIZACIÓN DE LA SEGURIDAD

11.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad, y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado/a de Protección de Datos (DPD).
- Responsable de la Información: Dirección de la AACID.
- Responsable del Servicio: Jefatura de Unidad.
- Responsable de Seguridad: Jefatura de Tecnología y Estrategia Digital.
- Responsable del Sistema: Jefatura de Tecnología y Estrategia Digital.

11.2. Comité de Seguridad Interior y Seguridad TIC de la AACID

La AACID ha constituido un Comité de Seguridad Interior y Seguridad TIC, como órgano colegiado, y está formado por los siguientes miembros:

- Presidencia del Comité de Seguridad Interior y Seguridad TIC: Dirección de la AACID.
- Vicepresidencia del Comité: Subdirección de la AACID.
- Vocales del Comité:
    - Jefatura de la Unidad de Cooperación con Iberoamérica de la AACID.
    - Jefatura de la Unidad de Cooperación con África y Mediterráneo de la AACID.
    - Jefatura del Departamento de Acción Humanitaria de la AACID.
    - Jefatura del Departamento de Buen Gobierno, Transparencia y Contratación de la AACID.
    - Persona designada como Responsable de Seguridad de la AACID.

  - Persona designada como Delegado/a de Protección de Datos de la AACID.
  - Persona designada como miembro de la unidad de seguridad interior de la AACID.
- Secretaría: Jefatura del Departamento de Buen Gobierno, Transparencia y Contratación de la AACID.

Con carácter opcional, otros miembros de la AACID podrán incorporarse como vocales asesores a las labores del Comité, incluidos grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Las personas designadas como vocales asesores participarán con voz, pero sin voto en las reuniones del Comité de Seguridad Interior y Seguridad TIC. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión de los vocales asesores.

El Comité de Seguridad Interior y Seguridad TIC celebrará sus sesiones en las dependencias de la AACID y/o de manera online, con periodicidad al menos anual, previa convocatoria al efecto realizada por la Presidencia de dicho Comité.

11.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del Responsable de la Información

La figura de Responsable de la Información recae en la Dirección de la AACID. Su cometido fundamental será establecer y aprobar los requisitos de protección de la información de la que la AACID es responsable, garantizar el cumplimiento normativo y asegurar la capacidad de la AACID para evidenciarlo.

De manera más detallada la persona designada como Responsable de la Información asume las siguientes funciones:

- El cumplimiento normativo relacionado con la Seguridad de la Información y la protección de datos personales.
- Establecer los requisitos de seguridad que deben ser garantizados por la AACID en el tratamiento de la información.
- Valorar los riesgos relativos a las dimensiones de seguridad (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información).
- Asegurar la implantación y el cumplimiento de los controles de seguridad que afecten a los servicios y áreas de la AACID.

Funciones del Responsable del Servicio

La figura de Responsable del Servicio asumirá las siguientes funciones:

- Valorar, para los servicios de los que son responsables, los riesgos relativos a las dimensiones de seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad).
- Velar por la correcta aplicación de los procedimientos y controles de seguridad en los servicios de los que son responsables.
- Trabajar en colaboración con el Responsable de Seguridad en el mantenimiento de los Sistemas bajo el alcance del ENS.
- Notificar a través del procedimiento de incidentes corporativo cualquier potencial problema de seguridad detectado en el servicio.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de Seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o el Comité de Seguridad Interior y Seguridad TIC.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad Interior y Seguridad TIC la aprobación de cambios y otros requisitos del sistema.

- Gestionar, supervisar y mantener la seguridad física de la AACID.
- Verificar que los controles y medidas de seguridad física establecidos son adecuados a las necesidades de la ACCID y los requisitos establecidos por la Dirección.

Funciones del Responsable del Sistema

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Implantar y gestionar los Sistemas de Información de la AACID durante todo su ciclo de vida, incluyendo la implantación de los controles de ciberseguridad, así como su operación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Asesorar y prestar soporte al Responsable de Seguridad en el desempeño de sus funciones, así como colaborar para la investigación y resolución de ciberincidentes que afecten a los Sistemas de Información de la AACID y aplicar el conocimiento obtenido del análisis de los ciberincidentes que hayan tenido lugar para reducir la probabilidad o el impacto de incidentes en el futuro.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Funciones del Comité de Seguridad Interior y Seguridad TIC

El Comité de Seguridad Interior y Seguridad TIC tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos 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.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar regularmente la Política de Seguridad para su aprobación por el órgano competente.

- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección.

- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de la Seguridad de la Información.

- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de Seguridad de la Información.

11.4. Procedimientos de designación

La creación del Comité de Seguridad Interior y Seguridad TIC, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por la Dirección de la AACID y comunicada a las partes afectadas.

Los miembros del Comité, así como los roles de seguridad serán revisados cada tres años o con ocasión de vacante.

12. RESOLUCIÓN DE CONFLICTOS

El Comité de Seguridad Interior y de Seguridad TIC de la AACID se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

13. DATOS DE CARÁCTER PERSONAL

La AACID solo tratará datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada momento.

De conformidad con 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 (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas

oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado/a de Protección de Datos.

14. TERCERAS PARTES

- Cuando preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad. La AACID definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que la AACID lleve a cabo en materia de Seguridad en relación con otros organismos.

- Cuando la AACID utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de las Normas de Seguridad existentes que atañen a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad establecidas en la disposición adicional segunda del Real Decreto 311/2022, y en consideración a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Responsable de la información y los Responsables de los Servicios afectados antes de seguir adelante.

15. MEJORA CONTINUA

La gestión de la Seguridad de la Información es un proceso sujeto a actualización permanente. Por ello, es necesario que la AACID implante un proceso de mejora continua que comportará entre otras acciones:

- Revisión de la Política de Seguridad.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas y externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de normas y procedimientos.

Para la AACID, la gestión adecuada de la Seguridad de la Información constituye un reto continuo y colectivo, necesario para la continuidad de la entidad.

La Directora de la Agencia Andaluza de Cooperación Internacional para el Desarrollo

Fdo.: Celia Rosell Martí