Responsable del documento: Jorge Juan Salamanca Fernández

Control de versiones

Versión	Motivo	Realizado por	Fecha
0.1	Versión preliminar. (Borrador)	Alaro Avant	22-02-2021
1.0	Versión inicial	Jorge Salamanca	23/03/2021
1.1	Versión revisada	Comité TIC, Director División Jurídico-Institucional	17/05/2021
2.0	Versión revisada para adaptar al nuevo ENS	Jorge Salamanca, Director División Jurídico-Institucional	20/07/2022
2.1	Pequeñas correcciones nuevo ENS	Jorge Salamanca, Director División Jurídico-Institucional	23/08/2023
	Revisado sin cambios	Resp. Seguridad	15-04-2024

Índice

Aprobado por: Comité Directivo de la AIReF, con fecha 23 de agosto de 2023

Introducción

Este documento expone la Política de Seguridad de la Información de la Autoridad Independiente de Responsabilidad Fiscal, AAI (en adelante AIREF), como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco del Esquema Nacional de Seguridad (ENS), y sustituye al documento Organización de la Seguridad TIC de la AIReF, vigente hasta la fecha.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la institución. Este activo debe ser adecuadamente protegido mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la calidad de la información y la continuidad de la actividad de la institución, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de la actividad de la institución.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la organización.

El Comité Directivo de la AIReF, consciente del valor de la información, está profundamente comprometido con la política descrita en este documento.

Definiciones

- **Sistema de Información:** conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.
- **Riesgo:** estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la

estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

- **Disponibilidad:** garantía de que los recursos del sistema se encontrarán operativos cuando se necesiten, especialmente los correspondientes a la información crítica.
- **Integridad:** disponibilidad de la información del sistema tal y como se almacenó por un agente autorizado.
- **Confidencialidad:** disponibilidad de la información solo para los agentes autorizados.
- **Autenticidad** (relativo al ENS): aseguramiento de la identidad u origen de la información.
- **Trazabilidad** (relativo al ENS): aseguramiento para ciertos datos de quién hizo qué y en qué momento.

Propósito

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información de la AIReF, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos de la institución y la legislación vigente.

Alcance

El alcance del Sistema de Gestión de Seguridad de la Información engloba los sistemas de información que soportan los procesos para servicios de evaluación, análisis y supervisión que se realizan en la AIReF ubicada en las oficinas de la c/José Abascal, 2-4, 2ª planta, Madrid, propiedad de la institución.

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la organización para los procesos descritos.

Están sujetas a esta política todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la AIReF. Por lo tanto, también se aplica a los contratistas, estudiantes en prácticas o cualquier otro tercero que tenga acceso a la información o a los sistemas de la organización.

Todas estas personas serán consideradas **usuarios** a los efectos del presente documento.

Para garantizar que el proceso de seguridad será actualizado y mejorado de forma continua, se implantará y documentará un Sistema de Gestión de la Seguridad de la Información. De esta forma, el contenido de la Política de Seguridad de la Información será desarrollado en normas y procedimientos complementarios de seguridad.

Objetivos y Fundamentos de esta Política

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción. Por ello, se establecen los siguientes principios mínimos:

a) Seguridad como proceso integral.

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. El tratamiento de la información estará presidido por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y de los responsables jerárquicos, para evitar que la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas constituyan fuentes de riesgo para la seguridad.

b) Gestión de la seguridad basada en los riesgos.

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, minimizando los mismos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

c) Prevención, detección, respuesta y conservación.

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar

o reducir la posibilidad de que las amenazas lleguen a materializarse. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

d) Existencia de líneas de defensa.

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

- Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

e) Vigilancia continua y reevaluación periódica.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

g) Diferenciación de responsabilidades.

En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales, además se identificará el responsable del tratamiento y, en su caso, el encargado del tratamiento.

Requisitos de Seguridad

Esta política de seguridad se desarrollará aplicando los siguientes requisitos:

Organización e implantación del proceso de seguridad.

La seguridad de la información compromete a todas las personas comprendidas en el ámbito de aplicación de este documento (usuarios). La AIReF identifica los responsables y establece sus responsabilidades al efecto en los apartados "Roles, responsabilidades y deberes" y "Terceras partes o terceros" de este documento. Esta Política de seguridad y la normativa serán conocidas por todas las personas comprendidas en el ámbito de aplicación de este documento.

Análisis y gestión de los riesgos.

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para la organización, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la LOPDGDD o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. El responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. Del resultado de ese análisis pueden derivarse medidas adicionales a implantar.

La AIReF utiliza la metodología **Magerit** para analizar los riesgos, realizando un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que queda recogido en un Documento de Análisis de Riesgos.

La entidad determina los niveles de riesgo a partir de los cuales adopta medidas para tratar los mismos. Un Riesgo se considera aceptable cuando implantar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Este análisis se repetirá:

- Regularmente, al menos cada una vez cada dos años.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

Una vez llevado a cabo el proceso de evaluación de riesgos y previo análisis y aprobación del Comité de Seguridad TIC, el Comité Directivo de la AIReF es el responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

Si el análisis de riesgos determina la necesidad de implantar medidas más severas que las implantadas en cumplimiento del ENS, se añadirán estas a las ya adoptadas.

Gestión de personal.

Todo el personal de la AIReF deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad, especialmente en los procedimientos de seguridad que en cada caso procedan. Sus actuaciones son supervisadas según los roles establecidos para verificar que se siguen los procedimientos definidos.

Los accesos de los usuarios son únicos y se verifican de forma periódica sus derechos y las actividades que tienen con la Seguridad de la información para corregir o exigir responsabilidades en su caso.

Profesionalidad, concienciación y formación.

La seguridad de los sistemas es gestionada por personal de la AIReF cualificado y personal externo especializado, que recibe y actualiza la formación necesaria para garantizar la seguridad de la información, siendo auditada por auditores externos.

El conjunto de Políticas, normas y procedimientos complementarios a esta Política de Seguridad de la Información también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se realizarán periódicamente actividades de concienciación y formación, y se entregará copia de la normativa correspondiente a los usuarios.

Autorización y control de los accesos.

El acceso a los sistemas de información es controlado, monitorizado y limitado a los usuarios, procesos, dispositivos y sistemas de información con las mínimas funcionalidades permitidas y/o autorizadas.

Protección física de las instalaciones.

Los sistemas de la AIReF están situados en áreas protegidas debidamente dotadas de medidas de seguridad físicas, de redundancia, continuidad y ambientales, y con un procedimiento de control de acceso.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Se adquirirán productos de seguridad y se contratarán servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información de forma proporcionada a la categoría del sistema y al nivel de seguridad determinado.

Siempre que sea posible, los productos o servicios deberán disponer de la correspondiente certificación de seguridad. En este sentido, el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- Otras certificaciones de seguridad adicionales que se requieran normativamente.
- Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el apartado de "Terceras partes" más adelante en este documento.

Mínimo Privilegio y Seguridad desde el Diseño.

En la AIReF los sistemas se diseñan y configuran siempre pensando en la Seguridad por Defecto. El sistema proporciona la mínima funcionalidad requerida porque las funciones de operación, administración y registro de actividad son las mínimas necesarias, y la AIReF se asegura de que solo son accesibles por las personas, y desde emplazamientos o equipos autorizados. Esto es particularmente importante en los sistemas de explotación, donde la AIReF elimina, desactiva, o aconseja desactivar o eliminar, según proceda, las funciones que no se vayan a utilizar.

Todos los proyectos relacionados o que afecten a los sistemas de información deberán incluir, en su proceso de análisis, una evaluación de los requisitos de seguridad y definir un modelo de seguridad consensuado con el responsable de seguridad de la información.

En el diseño, desarrollo, instalación y gestión de los sistemas de información y en los proyectos se tendrán en cuenta y aplicarán los conceptos de seguridad desde el diseño, codificación segura y los controles y medidas de seguridad que proceda según el documento de aplicabilidad aprobado por la organización.

Para ello, se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Integridad y actualización del sistema.

En la AIReF se comprueba la integridad y actualización de los sistemas de manera periódica para conocer en todo momento su estado de seguridad, tomando en consideración las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que procedan, y gestionando de esta manera la integridad de los mismos.

Todos los elementos de los sistemas requieren autorización previa a su instalación.

Protección de la información almacenada y en tránsito.

La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles.

La AIReF presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Esto incluye a la información almacenada o tratada en equipos portátiles, tabletas, smartphones, dispositivos periféricos, soportes de información, así como a las comunicaciones sobre redes abiertas o con cifrado débil, donde se aplican las medidas de seguridad que garanticen que la información se trata acorde a su clasificación.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica deberá estar protegida con el mismo grado de seguridad que esta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten procedentes.

Prevención ante otros sistemas de información interconectados.

La AIReF protege el perímetro de acceso a su sistema, en particular en las conexiones a través de Internet, analizando siempre los riesgos derivados de la interconexión con otros sistemas, y estableciendo las medidas que garanticen el nivel de seguridad necesario.

Registro de actividad.

La actividad de los sistemas de información y de sus usuarios queda registrada. Con el fin de asegurar la integridad y rendimiento de los sistemas de información y dispositivos digitales puestos a disposición de sus empleados para desarrollar sus funciones, se aplican las medidas previstas en la **Política de Garantía de Derechos Digitales**.

Incidentes de seguridad y detección de código dañino.

Cualquier compromiso de la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información de la AIREF se considera un incidente de seguridad.

La AIReF dispone de sistemas de detección y reacción frente a los incidentes de seguridad, que son clasificados y gestionados hasta su solución recopilando las evidencias de manera que se pueda informar y aprender de los mismos para mejorar de forma continuada.

En particular, la institución dispone de un sistema de detección y reacción frente a código dañino, así como de un sistema de prevención y detección de intrusiones, realizando auditorías técnicas para asegurar las medidas de protección pertinentes. Los usuarios disponen de canales establecidos para informar de forma inmediata de cualquier incidente o anomalía detectada.

Continuidad de la actividad de la institución.

La AIReF realiza las copias de seguridad que garantizan la recuperación de la información, y establece los mecanismos adecuados para asegurar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Mejora continua del proceso de seguridad.

El sistema de gestión de seguridad implantado es actualizado y mejorado de manera continua, según establecen las certificaciones de la norma ISO 27001 y el ENS.

Requisitos legales y marco normativo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- …
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

Así mismo, el Responsable de Seguridad será responsable de identificar las guías de seguridad del Centro Criptológico Nacional (CCN) que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

Roles, responsabilidades y deberes

El Comité Directivo de la AIReF asigna, renueva y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados, resolviendo los conflictos que se generen con relación a cada responsabilidad en Seguridad de la Información.

Usuarios

Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de la institución. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.
- Proteger y custodiar la información de la organización, evitando la revelación, emisión al exterior, modificación, borrado o destrucción accidental o no autorizadas o el mal uso independientemente del soporte o medios por los que se haya accedido a la misma o haya sido conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de las políticas, normas, procedimientos y medidas de seguridad aplicables.

Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en la normativa sobre régimen disciplinario de los empleados públicos o en los contratos que amparen su relación con la AIReF, sin perjuicio de la aplicación de la normativa sobre responsabilidad penal o civil que resulte procedente.

Responsable de la Información (ENS)

Es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

Tiene las siguientes responsabilidades:

- Velar por el buen uso de la información y, por tanto, de su protección, a través de la aprobación de la correspondiente política y normas de seguridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información tratada, valorando las consecuencias de un impacto negativo.

Responsable del Servicio (ENS)

Es el propietario de los activos del Servicio. Tendrá las siguientes responsabilidades generales:

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad, a través de la aprobación de la correspondiente política y normas de seguridad.
- Determinar las medidas de seguridad del servicio, de acuerdo con el Responsable de Seguridad y con el Responsable del Sistema, a través del Documento de Aplicabilidad.
- Velar por el mantenimiento de la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

Dirección

El Comité Directivo de la AIReF está profundamente comprometido con la política descrita en este documento y es consciente del valor de la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

En el contexto del ENS, el Comité Directivo asume las responsabilidades descritas para el Responsable de la Información y el Responsable del Servicio.

La Dirección es, por tanto, propietaria de los activos de información propios de la AIReF, y también responsable de los riesgos.

La Dirección asume, además, las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información

- Asegurar que se establecen la política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.
- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.
- Fomentar una cultura corporativa de seguridad de la información.
- Apoyar la mejora continua de los procesos de seguridad de la información.
- Asegurar que están disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información.
- Asegurar que se realizan auditorías de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.
- Definir y controlar el presupuesto para seguridad de la información.
- Aprobar la documentación hasta su segundo nivel de normas y procedimientos.
- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

Comité TIC

Con el fin de que toda la organización esté alineada con las directrices y necesidades de los sistemas de información, la AIReF dispone de un grupo formado por personal cualificado de las distintas Divisiones y del Gabinete de la Presidenta de la AIReF, denominado Comité TIC.

Las funciones del Comité TIC son las siguientes:

- Asesoramiento a la dirección en materia de Sistemas de Información y Comunicaciones.
- Foro de debate para la definición de estrategias relacionadas con los Sistemas de Información y Comunicaciones.
- Coordinación de proyectos TIC, transversales a la organización.
- Seguimiento del plan director de Sistemas de Información.
- Revisión de pliegos de contratación de servicios TIC.
- Atención a nuevas necesidades en materia de TIC.

Responsable de Seguridad (ENS)

Asumirá las siguientes funciones:

- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información, con la responsabilidad y autoridad para asegurarse de que el Sistema de Gestión de la Seguridad de la Información cumple con los requisitos del ENS.
- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.
- Implantar las medidas de seguridad establecidas por los Responsables del Servicio y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad.
- Realizar la coordinación y seguimiento de la implantación de los proyectos de adecuación a las normas especificadas (ISO 27001 y ENS), en colaboración con el Responsable del Sistema.
- Realizar, con la colaboración del Responsable del Sistema, los preceptivos análisis de riesgos, seleccionar las salvaguardas a implantar y revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable del Sistema, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información y analizar los informes de auditoría, elaborando las conclusiones a presentar al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
- Coordinar la Gestión de la Seguridad, en colaboración con el Responsable del Sistema.
- Elaborar informes anuales de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el Anexo II del ENS.
- Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
- Responder de la ejecución directa o delegada de las decisiones de la Dirección.

Respecto a la documentación, y apoyándose en el Responsable del Sistema, son funciones del Responsable de Seguridad:

- Proponer a la Dirección y al Responsable del Sistema para su aprobación la documentación de seguridad de segundo nivel (Normas de Seguridad TIC –STIC– y Procedimientos Generales del Sistema de Gestión de la Seguridad de la Información –SGSI–) y firmar dicha documentación.
- Aprobar la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).
- Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

Para el desarrollo de cualquiera de sus funciones el Responsable de Seguridad podrá recabar la colaboración del Responsable del Sistema.

Delegado de Protección de Datos.

Siguiendo lo indicado en el RGPD y en la LOPDGDD, el Delegado de Protección de Datos tendrá como mínimo las siguientes funciones:

- Informar y asesorar al responsable del tratamiento y a sus empleados de las obligaciones que les incumben con relación al RGPD y otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

Responsable del Sistema.

Las funciones del Responsable del Sistema son las siguientes:

- Desarrollar, operar y mantener el sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de 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.
- Realizar ejercicios y pruebas sobre los procedimientos operativos de seguridad y los planes de continuidad existentes.
- Realizar el seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, de acuerdo con el Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema, de acuerdo con el Responsable de Seguridad y la Dirección.
- Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de Seguridad y la Dirección.
- Realizar con la colaboración del Responsable de Seguridad, los preceptivos análisis de riesgos, seleccionar las salvaguardas a implantar y revisar el proceso de gestión del riesgo. Asimismo, junto al Responsable de Seguridad, aceptar los riesgos residuales calculados en el análisis de riesgos.
- Elaborar en colaboración con el Responsable de Seguridad, la documentación de seguridad de tercer nivel (Procedimientos Operativos STIC e Instrucciones Técnicas STIC).

El Administrador de la Seguridad del Sistema.

Las funciones que desempeñará son las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los procedimientos operativos de seguridad.
- La aplicación de los cambios de configuración del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los respectivos responsables de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Datos de Carácter Personal

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

En cumplimiento del RGPD y la LOPDGDD, se han ido adoptando medidas tales como: el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto cuando el riesgo ha sido alto, el registro de actividades de tratamiento y el nombramiento del Delegado de Protección de Datos.

De los análisis de riesgos que se realicen, se pueden derivar medidas que se superpongan a las ya adoptadas en cumplimiento del ENS, según la categorización del sistema.

Terceras partes o terceros

Cuando la institución preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. La AIReF definirá y aprobará los canales para la coordinación del suministro de información y de los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la AIReF utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad existente que atañe 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, los terceros deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el ENS cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el ENS, cuando se trate de sistemas de categorías MEDIA o ALTA, en los servicios concernidos.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se establece 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, que deberá ser aprobado por los Responsables de la Información y de los Servicios afectados.

Terceras partes como servicios externalizados de Seguridad

En el caso de servicios externalizados de seguridad, la entidad prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección de dicha entidad, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la entidad contratada, formará parte de su área o tendrá comunicación directa con la misma.

Revisión y Auditorías

El Responsable de Seguridad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen y la someterá, en su caso, a aprobación por el Comité Directivo.

Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de la actividad de la institución, prestando especial atención a las guías publicadas por el Centro Criptológico Nacional como desarrollo de las medidas y controles de seguridad.

La dirección será responsable de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a las situaciones de riesgo establecidas en el presente documento.

El sistema de gestión de seguridad se auditará cada dos años.