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 Diego Pérez Martínez Fecha: 2023.08.22 13:17:58 +02'00'

Índice

Aprobado por: Comité Directivo de la AIReF, con fecha 21 de mayo de 2021

Introducción

Este documento expone la Política de Seguridad de la Información de la Autoridad Independiente de Responsabilidad Fiscal (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 organización, 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 del negocio 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 Autoridad Independiente de Responsabilidad Fiscal ubicada en las oficinas de la c/ José Abascal, 2-4, 2ª planta, propiedad de la organización.

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, alumnos 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:

- **Principio de confidencialidad**: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

- **Principio de integridad y calidad**: se deberán establecer mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

- **Principio de disponibilidad y continuidad**: se dotarán los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

- **Principio de gestión del riesgo**: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

- **Principio de proporcionalidad en coste**: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos, sin perjuicio de que se asegurará que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles.

- **Principio de concienciación y formación**: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual manera, se exigirá la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

- **Principio de prevención**: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

- **Principio de detección y respuesta**: los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia respondiendo eficazmente, a través de los mecanismos establecidos al efecto, a los incidentes de seguridad.

- **Principio de mejora continua**: se revisará el grado de cumplimiento de los objetivos de mejora de la seguridad planificados anualmente y el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico de la Administración Pública.

- **Principio de seguridad TIC en el ciclo de vida de los sistemas de información**: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

- **Principio de función diferenciada**: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La Política de Seguridad de la Información es aprobada por el Comité Directivo de la AIReF, y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.

- Todos los usuarios con acceso a la información tratada, gestionada o propiedad de la organización tienen la obligación y el deber de custodiarla y protegerla.
- La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de la norma ISO/IEC 27001 y del Esquema Nacional de Seguridad.
- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad y se establecerá una planificación para su implantación y gestión.
- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.
- Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de

acuerdo con la normativa que resulte de aplicación y, en su caso, lo establecido en los contratos que amparen su relación con la AIReF.

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 el apartado de "Roles, responsabilidades y deberes" 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.

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.

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.

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 deberá 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.

Seguridad por defecto.

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.

Contratación y adquisiciones

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como no pública, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento del RGPD y de la LOPDGDD, así como de su normativa de desarrollo.

Las organizaciones y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las organizaciones y personas externas que accedan a la información de la organización deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

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.

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 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.

Cualquier compromiso de la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información de la organización 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 Esquema Nacional de Seguridad.

Requisitos Legales

- 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 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula 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 en 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 el que haya sido accedida o conocida.
- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

Responsable de la Información (Esquema Nacional de Seguridad)

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 (Esquema Nacional de Seguridad)

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 Esquema Nacional de Seguridad, 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

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 Esquema Nacional de Seguridad.
- 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 de Sistemas.
- 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 de Sistemas.
- Elaborar informes anuales de seguridad que incluyan los incidentes más relevantes en cada período, en coordinación con el Responsable de Sistemas.
- 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 de Sistemas 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 en 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. 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.

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.

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 año.