SI-01

Política de Seguridad de la Información

Contenido

1 Aprobación y entrada en vigor

La presente Política de Seguridad de la Información ha sido aprobada el día 15 de abril de 2024 por parte de la Dirección de SIMETRIA grupo[1] (en adelante SIMETRÍA o la Organización).

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Será revisada, junto a las propuestas de actualización o mantenimiento de la misma, con una periodicidad mínima anual.

El presente documento se trata de una versión extractada de la PSI al estar destinada a la comunicación externa a partes interesadas, por lo que se han eliminado las referencias que contengan información confidencial.

2 Introducción

SIMETRIA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad 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.

De este modo, todas las empresas de SIMETRIA, tienen presente que la seguridad es una parte integral de cada etapa del ciclo de vida de los sistemas TIC con que desarrollan sus

[1] *SIMETRÍA grupo está integrado por todas las Sociedades totalmente participadas por SIMETRÍA FIDENTIA, S.L., así como por aquellas entidades participadas mayoritariamente en las que ostente una posición de control en su gestión.*

funciones, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Mediante la presente Política, SIMETRIA ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), reconociendo como activos estratégicos la información que maneja, los servicios que presta y los sistemas TIC que soportan aquélla y hacen posible estos.

Esta Política protege a la información, servicios y sistemas TIC contra las amenazas existentes y persigue garantizar la continuidad operativa de aquéllos, minimizar los riesgos de daños que puedan sufrir y asegurar el eficiente cumplimiento de los objetivos de SIMETRIA.

Para ello, SIMETRIA, actuará preventivamente, supervisando la actividad diaria para detectar cualquier incidente, y reaccionará con presteza a las brechas de seguridad detectadas e incidentes cuando se produzcan, con la aplicación de las medidas de seguridad que en cada caso corresponda, entre otras las que se relaciona a continuación.

2.1 Prevención

SIMETRIA debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello deben implementarse las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, SIMETRIA:

- Autoriza los sistemas antes de entrar en operación.
- Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

SIMETRIA establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia, según lo dispuesto en el Artículo 10 del ENS (reevaluación periódica). Cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS Líneas de defensa), se

establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

2.3 Respuesta

SIMETRIA, establecerá las siguientes medidas:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados a las posibles partes interesadas (clientes, proveedores, grupos inversores, etc.).
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT) y con la Agencia Española de Protección de Datos.

2.4 Recuperación

Para garantizar la disponibilidad de los servicios, SIMETRIA dispondrá de los medios y técnicas que garanticen la recuperación de los servicios más críticos.

3 Alcance

El ámbito de aplicación de la presente Política abarca a todas las entidades que forman parte de SIMETRIA grupo ("SIMETRIA"), entendiéndose como tales todas las sociedades totalmente participadas por SIMETRÍA FIDENTIA, S.L. y las entidades participadas mayoritariamente en las que ostente una posición de control en su gestión.

Esta Política se aplica a los sistemas de información de SIMETRIA que dan soporte a los servicios de que se prestan dentro de la organización todo el personal que interviene de manera directa o indirecta en la prestación de dichos servicios, ya sea interno o externo a la organización.

4 Principios básicos de seguridad de la información

Los principios básicos son directrices fundamentales de seguridad que se tendrán presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico**: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de SIMETRIA, de forma que

pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

- **Responsabilidad determinada:** en los sistemas TIC se determinará 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 la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
- **Seguridad integral:** la seguridad se concibe y desarrolla como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.
- **Gestión de Riesgos:** el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** el establecimiento de medidas de prevención, detección, respuesta y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** las medidas de seguridad se evaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado, para lo que SIMETRIA podrá contar con el apoyo de servicios externos especializados.
- **Seguridad por defecto:** los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

5 Misión, visión y valores de la organización

- **Misión:** Diseñar, construir y gestionar de forma eficiente Infraestructuras y Servicios basados en la Sostenibilidad, la Innovación y la creación de Valor para nuestros Grupos de Interés.

- **Visión:** Dirigir nuestras actividades hacia el desarrollo de un futuro sostenible, afianzando la excelencia y la honestidad como señas de identidad, y teniendo por máxima el planeta, las personas y la solvencia y rentabilidad que avalen la continuidad del Grupo.

Valores Corporativos

- **Experiencia:** La experiencia en las actividades que desarrollamos nos lleva a trabajar con ejemplaridad y vocación de servicio hacia nuestros clientes, desarrollando la capacidad de los equipos y apostando por la formación y especialización de las personas, siendo nuestra forma de generar proyectos de gran Profesionalidad, lo cual repercute directamente en la reputación e imagen del Grupo. Por ello mostramos un comportamiento honrado, basado en la honestidad, con el fin de generar un sentimiento de Lealtad, lo que consideramos un valor tan atractivo como gratificante.

  La seguridad de las personas constituye un eje estratégico de nuestras decisiones, por ello, el mantenimiento de altos estándares de seguridad y nuestro Plan interno de Seguridad y Salud forman una parte irrenunciable de nuestros procesos.

- **Vocación de Servicio:** Los colaboradores de SIMETRÍA GRUPO atenderán los intereses de los clientes a través de la implicación y del compromiso laboral, contribuyendo positivamente a la eficiencia, productividad, satisfacción y éxito de la organización y velando por cumplir adecuadamente los proyectos desarrollados. Trabajamos con el objetivo de obtener relaciones de larga duración, ofreciendo un servicio de calidad y proximidad, y apostando por la formación y especialización de las personas que componen nuestros equipos, y destacando el Compromiso y Adaptabilidad.

- **Sostenibilidad:** Trabajamos para que la sociedad y el desarrollo sean sostenibles, mejorando el bienestar con infraestructuras y servicios. Tenemos en cuenta todos los ámbitos de la sostenibilidad, siendo solventes económicamente desde hace más de 80 años, generando empleo de calidad y bienestar personal, basándonos en el Respeto hacia las personas y trabajando en reducir el impacto ambiental de nuestras actividades, todo ello alineado con la Agenda 2030 de Naciones Unidas y sus Objetivos de Desarrollo Sostenible.

- **Innovación:** Buscamos constantemente la mejora. Por ello incentivamos la creatividad y la generación de nuevas ideas, aplicando la mejor tecnología disponible en cada momento e innovamos en el desarrollo de nuestros procesos, servicios y productos, con el objeto de adelantarnos a las necesidades de nuestros clientes y de la sociedad, y apostando por potenciar la Economía Circular, la

Eficiencia y la Protección del Medioambiente, progresando en la sostenibilidad de nuestras actividades.

6 Objetivos

Con el fin de garantizar la protección efectiva de la información y de los recursos corporativos necesarios para el correcto funcionamiento de los servicios prestados por SIMETRIA, tanto de amenazas externas como internas y definiendo dicha protección en términos de calidad y seguridad, se establecen los siguientes objetivos y principios básicos:

- Cumplir los requisitos legales y contractuales aplicables al desarrollo de sus funciones en la organización y la protección de datos de carácter personal y la continuidad de los procesos de negocio.
- Difundir entre todo el personal la necesidad y obligatoriedad de cumplir y hacer cumplir las políticas y normativas aplicables en materia de seguridad de la información, individualmente en función de sus tareas dentro de la organización.
- Restringir el uso tanto de la información en sí como de los sistemas que la procesan a aquellas tareas necesarias para el correcto desempeño del trabajo de cada persona, estando prohibido el uso en beneficio particular de ningún activo de SIMETRIA.
- En el caso de la información, considerada como uno de los activos principales de SIMETRIA, es deber de todo el personal mantener el secreto respecto a la misma y no divulgarla a terceros, salvo que las comunicaciones formen parte imprescindible de la relación laboral y en cumplimiento de las debidas garantías de confidencialidad establecidas.

7 Marco normativo y legal

El marco normativo en que se desarrollan las actividades de SIMETRIA y, en particular, la prestación de sus servicios de tecnologías de la información está integrado por las siguientes normas:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.

- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 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.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

8 Organización de la seguridad

8.1 Criterios utilizados para la Organización de la Seguridad de la Información

SIMETRIA, teniendo en cuenta lo establecido en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y las pautas establecidas en la Guía CCN-STIC-801 "Responsabilidades y Funciones en el ENS", para organizar la seguridad de la información emprenderá las siguientes acciones:

- **Designará roles de seguridad:** Responsables de Servicios, Responsables de Información, Responsable de Seguridad de la Información, Responsable del Sistema.
- **Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información.** Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

8.2 Comité de Seguridad

Con el fin de facilitar la gestión de la seguridad en SIMETRIA, la Dirección aprueba mediante la presente política, la conformación de un Comité de Seguridad de la Información (en adelante CSI), dedicado a la gestión y coordinación de todas las actividades relacionadas con la seguridad de los sistemas de información en la organización, ejerciendo las siguientes funciones:

- Aprobar las propuestas de modificación y actualización permanente de la PSI.
- Aprobar las Normativas y Procedimientos de Seguridad de la información que puedan derivar de la Política de Seguridad.
- Velar e impulsar el cumplimiento de la PSI, así como su desarrollo normativo.
- Atender las inquietudes en materia de seguridad de la información de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua en la gestión de la seguridad de la información.
- Impulsar la formación y concienciación.
- Resolver los conflictos que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Analizar los informes facilitados por el responsable de seguridad relativos al resultado de los análisis de riesgos, de las auditorías realizadas, de los proyectos y de las iniciativas y acciones de mejora de la seguridad requeridas.

Revisar la información aportada por el responsable de seguridad de la información relativa a los incidentes de seguridad.

El Comité de Seguridad de la Información está compuesto por los siguientes miembros:

- **Presidente**: La dirección general de SIMETRIA
- **Secretario:** Responsables de seguridad de SIMETRIA y CASVA SEGURIDAD
- **Vocales:** Responsables de la información y servicios de todas las empresas de SIMETRIA identificados en el ámbito de la presente política.

El CSI se reunirá con carácter ordinario, al menos, una vez al año. Por razones de urgencia podría reunirse cuando su presidente lo establezca.

8.3 Roles y responsabilidades en materia de seguridad

Además del Comité de Seguridad de la Información, cuyas funciones y responsabilidades se han mencionado anteriormente, a continuación, se indican las del resto de roles implicados.

- **Responsables de Seguridad**
- **Responsables del Sistema**

- **Responsables del Servicio**
- **Responsables de la Información**

8.3.1 Responsable de Seguridad

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- 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 de la información.
- 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 Comité de Seguridad de la Información de la Información.
- Participará 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 la aprobación de cambios y otros requisitos del sistema.
- En caso de ciberataque de especial gravedad o cuando detecte deficiencias o brechas de seguridad que entienda supongan grave riesgo para los objetivos que la presente política pretende alcanzar, impulsará las acciones correctoras que estime necesarias, incluso mediante contratación de emergencia, dando cuenta de las mismas al Comité de Seguridad de la Información en la siguiente sesión que celebre.

En el desempeño de sus funciones, el Responsable de Seguridad de la Información contará con el apoyo de técnicos dentro del ámbito TIC y/o de servicios externos especializados.

8.3.2 Responsable del Sistema

Serán 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.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Elaborando los procedimientos operativos necesarios.
- Definir la tipología 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.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- 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.
- Informar al Responsable de Seguridad 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.

8.3.3 Responsable del Sistema Delegado

Debido a la casuística diferenciada que presenta CASVA dentro de SIMETRÍA, se ha identificado la necesidad de contar con un rol adicional que se enfoque exclusivamente en los aspectos particulares de CASVA.

El Responsable de Sistema Delegado opera dentro del ámbito de los servicios específicos asignados por el Responsable del Servicio. Aunque se le confiere la potestad de llevar a cabo funciones operativas esenciales, es importante destacar que la responsabilidad última sigue siendo del Responsable del Servicio.

8.3.4 Responsable de la Información

El Responsable de la Información (information owner) tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección; es el responsable último de cualquier error o negligencia que lleve a un incidente de seguridad. Tiene la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

Dentro de su ámbito de actuación, tendrá las siguientes funciones:

- Determinar los requisitos de seguridad de la información que tratan.
- Validar y aceptar el riesgo residual resultante del análisis de riesgos.
- Validar la normativa para el tratamiento de la información de la cual es responsable.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto a la Información de los que es responsable, especialmente la incorporación de nueva Información a su cargo.
- Impulsar y perseguir la consecución de la seguridad de la información dentro del ámbito de sus competencias.

El Responsable de la Información puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).

Aunque la aprobación formal de los niveles de seguridad corresponda al Responsable de la Información, se podrá recabar una propuesta al Responsable de la Seguridad y se considerará la opinión del Responsable del Sistema.

8.3.5 Responsable del Servicio

El Responsable del Servicio tiene la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.

El Responsable del Servicio deberá establecer los requisitos de los servicios en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad. El Responsable del Servicio determinará los niveles de seguridad de los servicios.

Dentro de su ámbito de actuación, tendrá las siguientes funciones:

- Determina los requisitos de seguridad de los servicios prestados.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Validar y aceptar el riesgo residual resultante del análisis de riesgos.
- Poner en comunicación del Responsable de Seguridad cualquier variación respecto al servicio o servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo.
- Validar la normativa para la prestación del servicio del cual es responsable.

El Responsable del Servicio puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se podrá recabar una propuesta al Responsable de la Seguridad y se considerará la opinión del Responsable del Sistema.

8.4 Procedimiento de designación y renovación

Los roles y responsabilidades en materia de seguridad de la información serán designados por la Dirección de SIMETRIA a propuesta del Comité de Seguridad de la Información. De igual forma, la Dirección es la encargada de la designación de los distintos miembros que formarán el Comité de Seguridad de la Información.

Asimismo, la Dirección se reserva el derecho de la revisión y renovación de las asignaciones y responsabilidades en cualquier momento.

9 Datos de carácter personal

SIMETRIA recogerá los datos de carácter personal adecuados, pertinentes y no excesivos y sólo cuando se hallen 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.

10 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis de riesgos, identificando las amenazas y evaluando los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.

El Responsable de Seguridad de la Información ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.
- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos, como norma general se utilizará la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica.

11 Obligaciones del personal

Todo el personal de SIMETRIA, interno o externo, que utilice o tenga acceso a la información y/o a los sistemas tecnológicos o de información corporativos, tiene las siguientes obligaciones:

- Conocer, cumplir y hacer cumplir esta Política de Seguridad de la Información y las Normativas de Seguridad y procedimientos que la desarrollan y que le afecten.
- Atender a las acciones de concienciación en materia de seguridad de la información que se realicen.
- Utilizar los servicios y sistemas de información, así como la información en ellos contenida y a la que tengan acceso, con una finalidad profesional acorde a las tareas encomendadas en función de su puesto de trabajo y a los fines y propósitos que motivaron la concesión del acceso.
- Velar por la confidencialidad de la información a la que tenga acceso según la clasificación y características de la misma.
- Notificar eventos que puedan suponer una brecha de seguridad o evidencien una debilidad que pueda implicar posteriores brechas.
- Colaborar en la resolución de brechas de seguridad y en la realización de acciones preventivas cuando sea necesaria su participación
- Participar en la estructura de gestión de la seguridad de la información cuando corresponda según las competencias y funciones de su puesto de trabajo.
- No realizar acciones intencionadas o negligentes que puedan perjudicar la seguridad de los sistemas tecnológicos o la información que contienen.

Asimismo, queda bajo la responsabilidad de los usuarios hacer un uso proporcional, adecuado y justificado de los medios puestos a su disposición para el desarrollo de sus funciones. Cualquier uso indebido, podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

12 Desarrollo de la política de seguridad de la información

La presente Política de Seguridad de la Información será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas).

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada documento de un determinado nivel de desarrollo se fundamente en los documentos de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

1. Primer nivel normativo: Constituido por la presente Política de Seguridad de la Información.
2. Segundo nivel normativo: Constituido por el conjunto de normas que complementan la política y uniformizan la utilización de aspectos concretos del sistema de información, indicando su uso correcto y las responsabilidades de los diferentes usuarios, técnicos y administradores.
3. Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la Política de Seguridad de la Información, determinan las acciones o tareas a realizar en el desempeño de un proceso.

El Comité de Seguridad de la Información de SIMETRIA se responsabiliza de que este conjunto de documentos que forman parte del sistema documental de SIMETRIA sean revisados con una periodicidad mínima anual y, si procede, actualizados siempre que sea necesario.

Esta normativa de seguridad estará a disposición, y fácilmente accesible, de todos los miembros de la organización que necesiten conocerla.

13 Relación con terceros

Cuando SIMETRIA preste servicios a otras organizaciones o maneje información de otras organizaciones, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos comités de seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SIMETRIA utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información y de las Normativas de Seguridad aplicables a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

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

14 Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

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