Política de Seguridad de la Información

Lo mejor de las TIC con un toque humano

Control del Documento

Política de Seguridad de la Información	Nombre	Fecha
Redactado por	Resp. Seguridad de la Información/ Resp. Seguridad Corporativa	23/09/2024
Revisado por	Comité de Seguridad	10/10/2024
Aceptado por	Comité de Dirección	10/10/2024

Versión del documento

Versión	Fecha	Cambio
v.5.0	05/12/2023	Revisión y actualización completa del documento
v.5.1	10/10/2024	Cumplimiento de políticas y auditorías

Derechos de propiedad

ÍNDICE

1. ALCANCE

Teniendo en cuenta el contexto de AXIANS para el SGSI, en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, AXIANS ha establecido el siguiente Alcance:

"Los Sistemas de Información que dan soporte a los servicios prestados desde el Centro de Servicios Gestionados de Red (NOC), Seguridad (SOC), Sistemas (DOC) y Voz y vídeo (VOC) para las siguientes actividades:

- Monitorización
- Service Desk
- Análisis y Operación
- Soporte"

2. DEFINICIONES Y ABREVIATURAS

Las definiciones relacionadas con los estándares ISO pueden consultarse en:

https://www.iso.org/obp/ui

A continuación, se indican las abreviaturas que aplican a este documento:

ABREVIATURA	DEFINICIÓN
ENS	Esquema Nacional de Seguridad
PSI	Política de Seguridad de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
IT	Information & Tecnology
CSO	Responsable de Seguridad Corporativa
BU	Business Unit (Unidad de Negocio)

3. RESPONSABILIDADES

Las responsabilidades del presente documento quedan definidas en la descripción de cada apartado.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1. Objetivos y misión de la organización (la estrategia y los requisitos del negocio)

ENS [org.1.1] ; ISO27001 [A.5.1]

Acuntia, S.A.U. opera en el mercado a través de la marca AXIANS, que pertenece al Grupo VINCI. AXIANS es una organización especializada en las tecnologías de la información y las comunicaciones, que proporciona un amplio espectro de soluciones y servicios para atender las necesidades de las empresas en infraestructuras IT y comunicaciones.

AXIANS es el nexo de nuestro planeta conectado. Aspiramos a algo más que a la excelencia técnica, a hacer que el mundo de mañana sea más habitable y justo. Formamos parte de un Grupo impregnado de sólidos valores humanos y ética social, una cultura de relaciones cualitativas y una estrecha atención a las partes interesadas y los usuarios finales.

Para cumplir con nuestro propósito AXIANS ha desarrollado esta Política conforme al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), al estándar ISO 27001:2022 y a la legislación aplicable, con el objetivo principal de proteger los intereses de la compañía y de sus clientes y el fin de asegurar la seguridad y la confianza mediante la prestación de servicios que cumplan estos requisitos.

Para AXIANS, la seguridad se convierte en uno de sus objetivos principales, la cual permite garantizar la confidencialidad, privacidad, disponibilidad, integridad, autenticidad y trazabilidad de los servicios que proporciona, a través del establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI).

4.1.1. Objetivos de seguridad de la información

Los objetivos de seguridad se planifican y establecen de forma que se garantice el cumplimiento de las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) y la norma UNE-EN ISO/IEC 27001, en su versión vigente, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas

y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

4.1.2. Principios de seguridad

En este contexto, AXIANS trata la información y los datos personales bajo su responsabilidad, conforme a los principios y requisitos recogidos en los diferentes marcos normativos que le son de aplicación y los que serán desarrollados e implementados a través de la presente Política de Seguridad y su desarrollo normativo.

En cumplimiento con lo establecido en el *Artículo 12 del RD 311/2022* esta política de seguridad de la información es el conjunto de directrices que rigen la forma en que AXIANS gestiona y protege la información que trata y los servicios que presta, de acuerdo con los siguientes principios básicos, que se rigen por el *Artículo 5 del RD 311/2022* y que guían permanentemente nuestra actuación en este ámbito:

- Seguridad como proceso integral
- Gestión de la seguridad basada en los riesgos
- Prevención, detección, respuesta y conservación
- Existencia de líneas de defensa
- Vigilancia continua
- Reevaluación periódica
- Diferenciación de responsabilidades

4.2. Marco Legal y regulatorio en el que se desarrollan las actividades

ENS [org.1.2] ; ISO27001 [A.5.31]

El marco legal y regulatorio en el que se desarrollan nuestras actividades viene determinado por:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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 Comercio Electrónico.
- 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- Resolución de 27 de febrero de 2023, de la Dirección General de Trabajo, por la que se registra y publica el XX Convenio colectivo nacional de empresas de ingeniería; oficinas de estudios técnicos; inspección, supervisión y control técnico y de calidad.
- Ley 31/1995, de 8 de noviembre de prevención de riesgos laborales.
- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.
- Ley 11/2022, de 2 de junio de 2022, General de Telecomunicaciones.
- Real Decreto 244/2010, de 5 marzo, por el que se aprueba el Reglamento regulador de la actividad de instalación y mantenimiento de equipos y sistemas de telecomunicación.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y su normativa de desarrollo (Real Decreto 43/2021, de 26 de enero).

4.2.1. Otras Normativas

- UNE-EN ISO/IEC 27001:2022, Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 27002: 2022, Information technology. Security techniques. Code of practice for information security controls.

4.3. Roles y funciones de seguridad

ENS [org.1.3] ; ISO27001 [A.5.2] [A.5.3]

4.3.1. Dirección de AXIANS

La Dirección es la figura de la que depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.

La Dirección de AXIANS es responsable de las siguientes funciones:

- Fijar los objetivos estratégicos
- Organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas y dirigir su actividad
- Aprobar la Política de Seguridad de la Información y la Política de Protección de Datos
- Facilitar los recursos adecuados para alcanzar los objetivos propuestos
- Velar por su cumplimiento de la Seguridad de la Información

4.3.2. Responsable de la Información y del Servicio

El Responsable de la Información y del Servicio es designado por la Dirección de AXIANS, según el procedimiento descrito en esta PSI.

En AXIANS, ambas responsabilidades se encuentran unificadas, coincidiendo en el mismo rol, de forma habitual.

El Responsable de la Información y del Servicio es la persona que tiene la potestad y la responsabilidad de:

- Establecer los requisitos de la información en materia de seguridad
- Determinar y aprobar los niveles de seguridad de la información en cada dimensión de seguridad, pudiendo recabar una propuesta por parte del Responsable de Seguridad y siendo conveniente que escuche la opinión del Responsable del Sistema
- El uso que se haga de la información y, por tanto, de su protección
- Sobre 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)
- La prestación del servicio siempre atienda a los requisitos de seguridad de la información que maneja, a los que se suele añadir requisitos de disponibilidad, accesibilidad, interoperabilidad, etc.

- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios y de la información atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos
- La determinación de los niveles en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad

4.3.2.1. Responsable de la Seguridad de la Información

El Responsable de la Seguridad de la Información es designado por la Dirección de AXIANS, según el procedimiento descrito en esta PSI.

Según lo señalado en el ENS, el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Siendo sus dos funciones esenciales:

- Mantener la seguridad de la información manejada, y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la presente PSI
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad

Además de ello, asume las siguientes funciones:

- Elaborar y proponer, para aprobación por la organización, las políticas de seguridad que incluyan las medidas técnicas y organizativas adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados, y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad
- Elaborar el documento de Declaración de Aplicabilidad
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos
- Constituirse como punto de contacto con la autoridad competente, en materia de seguridad de las redes y sistemas de información, y ser responsable ante aquella del

cumplimiento de las obligaciones que se derivan del RD 12/2018 y de su Reglamento de Desarrollo

- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas
- Recopilar, preparar y suministrar información o documentación a la autoridad competente, o el CSIRT de referencia, a su solicitud o por propia iniciativa

4.3.2.2. Responsables de Seguridad de la Información delegados

Si en los sistemas de información, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesita de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, AXIANS puede designar Responsables de Seguridad Delegados. La designación corresponde al Responsable de la Seguridad, que delegará funciones, no responsabilidad.

Los Responsables de Seguridad Delegados se harán cargo, en su ámbito competencial, de todas aquellas funciones delegadas por el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos (departamentales, por ejemplo) o de sistemas de información horizontales.

Cada Responsable de la Seguridad Delegado mantendrá una dependencia funcional directa del Responsable de la Seguridad, a quien debe reportar.

4.3.3. Responsable del Sistema

El Responsable del Sistema es designado por la dirección de AXIANS y su posición figura en la presente PSI.

El Responsable del Sistema tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad

El Responsable del Sistema puede proponer la suspensión del tratamiento de una cierta información, o la prestación de un determinado servicio, si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por el Comité de Seguridad de AXIANS, debe ser acordada con los Responsables de la Información y los Servicios afectados y el Responsable de Seguridad de la Información.

4.3.3.1. Responsables del Sistema delegados

Si en el sistema de información, por la complejidad, distribución, separación física de sus elementos o número de usuarios, se necesita de personal adicional para llevar a cabo las funciones de Responsable del Sistema, AXIANS podrá designar cuantos Responsables del Sistema Delegados considere necesarios. La designación corresponde al Responsable del Sistema, que delega funciones, no responsabilidad.

Los Responsables del Sistema Delegados se harán cargo, en su ámbito competencial, de todas aquellas acciones delegadas por el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

Cada Responsable del Sistema Delegado mantendrá una dependencia funcional directa del Responsable del Sistema, a quien reportarán.

4.3.4. Administrador de seguridad

El Administrador de Seguridad (AS) es designado por la dirección de AXIANS y depende del Responsable del Sistema.

Sus funciones más significativas 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 del sistema de información
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado
- La aplicación de los Procedimientos Operativos de Seguridad (POS)
- Asegurar que los controles de seguridad establecidos son adecuadamente observados
- 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 al Responsable de la Seguridad o al Responsable del Sistema 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

4.3.4.1. Administradores de Seguridad delegados

Si en los sistemas de información, por su complejidad, distribución, separación física de sus elementos o número de usuarios, se necesita de personal adicional para llevar a cabo las funciones de Administrador de Seguridad, AXIANS puede designar Administradores de Seguridad Delegados.

Los Administradores de Seguridad Delegados serán responsables, en su ámbito competencial, de aquellas acciones que delegue el Administrador de Seguridad relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

El Administrador de Seguridad Delegado será designado a solicitud del Administrador de Seguridad, del que dependerá funcionalmente.

4.3.5. Responsable de seguridad física

En AXIANS, las medidas de protección de las instalaciones físicas se clasifican en:

- Obstáculos físicos (accesos físicos, tornos, puertas, candados, etc.);
- Técnicas de vigilancia (sistemas de alarma, técnicas de vigilancia y monitorización);
- Sistemas de inteligencia (herramientas de análisis y simulación de información basados en los datos extraídos de la monitorización);
- Vigilantes y personal de seguridad

AXIANS contempla los requisitos y medidas de seguridad necesarios para el desarrollo de su actividad, y ha establecido un marco de referencia para dar respuesta a las exigencias de seguridad tanto físicas como lógicas.

El Responsable de la Seguridad Física debe adoptar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de la Seguridad de la Información, e informar a éste de su grado de implantación, eficacia e incidentes.

En AXIANS las responsabilidades en materia de Seguridad de la Información y la Seguridad física relacionada, son asumidas por el mismo rol, el responsable de Seguridad Corporativa (CSO).

4.3.6. Responsable de gestión del personal

Las áreas responsables de la gestión del personal de AXIANS deben adoptar las medidas de seguridad que le competan en materia de seguridad ligada al personal, dentro de las determinadas por el Responsable de la Seguridad de la Información, e informar a este de su grado de implantación, eficacia e incidentes.

4.3.7. Responsables del Tratamiento

El Responsable del Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento.

El Responsable del Tratamiento debe asumir las obligaciones y responsabilidades establecidas en el marco normativo de protección de datos aplicable, contando con el asesoramiento de los

Delegados de Protección de Datos asignados o con aquella figura de responsabilidad designada en su defecto.

4.3.8. Encargados del Tratamiento

La persona designada como Encargado del Tratamiento de datos personales es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata datos personales por cuenta de la persona designada Responsable del Tratamiento o figura de responsabilidad designada en su defecto.

La condición de Encargado del Tratamiento supone la asunción de las obligaciones y responsabilidades establecidas para dicha figura en el marco normativo de protección de datos aplicable, contando con el asesoramiento de los Delegados de Protección de Datos asignados o figura de responsabilidad designada en su defecto.

4.3.9. Responsable de protección de datos y compliance

El Responsable de Protección de Datos y Compliance es la figura designada en AXIANS para tratar las cuestiones referidas habitualmente al Delegado de Protección de Datos.

Entre otras funciones, se destaca:

- Informar y asesorar a la organización y los empleados que se ocupan del tratamiento de datos personales de sus obligaciones
- Controlar que la organización responde a sus obligaciones de cumplimiento, así como a las disposiciones y políticas internas, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes
- Organizar la realización de revisiones periódicas del conjunto de medidas técnicas y organizativas relacionadas con la protección de datos personales
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto, relativa a la protección de datos, y supervisar su aplicación
- Actuar como punto de contacto de la Autoridad de Control y cooperar con esta en cuestiones relativas a los datos personales, en su caso

4.3.10. Designación y renovación de roles y funciones

- Responsable de la Información, que puede ser un cargo unipersonal o un órgano colegiado será designado dentro de la organización de la unidad de negocio o similar.
- Responsable del Servicio, que, pudiendo ser el mismo que el Responsable de la Información, también puede ser un cargo unipersonal un órgano colegiado será designado dentro de la organización de la unidad de negocio o similar.
- Responsable de la Seguridad, que debe reportar directamente a la Dirección o a los órganos de gobierno de la entidad y, cuando existan, a los Comités de Seguridad y de Seguridad de la Información. Será designado por la Dirección.
- Responsable del Sistema, que, en materia de seguridad, reporta al Responsable de la Seguridad. Esta designación puede ser:
  - ✓ A propuesta del Responsable de la Información tratada, cuando el Sistema de Información trate una única información
  - ✓ A propuesta del Responsable del Servicio prestado, cuando el Sistema de Información preste un único servicio
  - ✓ Directamente, cuando el Sistema de Información trate diferentes informaciones o preste diferentes servicios, escuchados los responsables de las informaciones y los servicios afectados
- Administrador de Seguridad, a propuesta del Responsable del Sistema

El procedimiento para la designación y renovación de los roles descritos anteriormente consiste en la ratificación en el Comité de Seguridad de AXIANS, órgano ejecutivo y con autonomía para la toma de decisiones y que no subordina su actividad a ningún otro elemento de nuestra empresa, excepto al Comité de Dirección.

Este Comité de Seguridad es el órgano con mayor responsabilidad dentro del Sistema de Gestión de Seguridad de la Información, tomando todas las decisiones relevantes relacionadas con la misma, y quedando sus decisiones reflejadas en las actas.

Los roles designados se renuevan anualmente de forma automática. Las bajas o modificaciones en dichos roles se comunican al Comité de Seguridad de AXIANS, siguiendo los cauces establecidos para la designación de los nuevos roles.

4.3.11. Registro de roles y funciones

Los roles y funciones definidos anteriormente se registran y mantienen en la herramienta GRC, para lo cual se realiza una revisión periódica, al menos anualmente o cuando haya un cambio significativo.

4.4. Estructura del comité o comités para la gestión y coordinación de la seguridad

ENS [org.1.4] ; ISO27001 [A.5.4]

La estructura organizativa para la gestión de la seguridad, en los ámbitos de la presente Política, está compuesta por los siguientes órganos y agentes:

4.4.1. Comité de Seguridad

El Comité de Seguridad se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, compliance (seguridad y conformidad legal) y planes de contingencia.

El Comité de Seguridad, está formado por:

- Un miembro de la Dirección de AXIANS
- El Responsable de Seguridad Corporativa
- El Responsable de Seguridad de la Información
- El Responsable del Sistema
- La Responsable de RRHH (miembro no permanente con asistencia discrecional)
- La Responsable de Legal, Protección de datos y Compliance
- El Responsable del Sistema de Gestión de la Seguridad de la Información
- El Gerente de Sistemas IT
- El Coordinador de Sistemas IT

Entre las funciones del Comité de Seguridad se encuentran:

- Elaborar (y revisar regularmente) la Política de Seguridad de la Información, para su aprobación por la Dirección

- Definir, dentro de la Política de Seguridad, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación
- Aprobar la Normativa de Seguridad de la información
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular, debe velar por la coordinación de distintos planes que puedan realizarse en diferentes áreas
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes y están alineados con la estrategia decidida en la materia, evitando duplicidades
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en el caso de ser activados
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes
- Recabar del Responsable de Seguridad de la BU informes regulares del estado de la seguridad de la BU y de los posibles incidentes
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC, desde su especificación inicial hasta su puesta en operación. En particular, debe velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas por los diferentes ámbitos de seguridad, encargándose de gestionar un control y presentación regular de los proyectos y un anuncio de las posibles desviaciones

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados
- Recibir inquietudes en materia de seguridad de la Dirección y transmitirlas a los Responsables de las BU pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, son comunicadas a la Dirección
- Coordinar y dar respuesta a las inquietudes transmitidas a través del Responsable de Seguridad de la BU
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información
- Resolver los conflictos de responsabilidad 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

El Responsable de la Seguridad Corporativa (CSO) actúa como Secretario del Comité de Seguridad y entre sus cometidos se encuentran:

- Convocar al Comité de Seguridad, recopilando la información pertinente
- Recabar las inquietudes de la Dirección de AXIANS y del Responsable de Seguridad de la BU, incorporándolas al Orden del Día del Comité de Seguridad, para su examen y acciones pertinentes
- Es responsable, junto con el Responsable de Seguridad de la BU, de estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al Comité de Seguridad y proponiendo las medidas oportunas de adecuación al nuevo marco
- Es el responsable de la toma de decisiones cotidianas entre las reuniones del Comité de Seguridad. Estas decisiones deben dar respuesta a propuestas del Responsable de Seguridad de la BU, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres

Suele ser habitual que el Responsable de la Seguridad Corporativa se incorpore al Comité de Crisis en caso de desastre, coordinando todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la organización.

4.4.1.1. Periodicidad de las reuniones y adopción de acuerdos

El Comité de Seguridad se reúne, al menos, trimestralmente, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones o una convocatoria discrecional.

En cualquier caso, las reuniones se convocan por su Presidencia, a través del secretario, a su iniciativa o por mayoría de sus miembros permanentes.

Las decisiones serán adoptadas por consenso de los miembros.

4.4.2. Grupos de Trabajo Técnico de Seguridad

Dentro de la estructura de gobierno de AXIANS, para la Seguridad de la Información se establecen grupos de trabajo que dan apoyo al Comité de Seguridad mediante la gestión y coordinación de las actuaciones en materia de seguridad.

4.4.2.1. Grupo de trabajo de Gobierno de la Seguridad

Este grupo de trabajo está compuesto por:

- El Responsable de Seguridad Corporativa
- El Responsable de Seguridad de la Información (asistirá a las reuniones en función de la necesidad de los temas tratados)
- El Responsable del Sistema
- El Responsable del Sistema de Gestión de la Seguridad de la Información
- Los técnicos del Sistema de Gestión de la Seguridad de la Información
- El Coordinador de Sistemas IT
- Un técnico del área de Infraestructura IT

Dentro de las funciones asociadas a este grupo de trabajo, se destacan las siguientes:

- Colaborar en el aseguramiento de que el SGSI es conforme con los requisitos de las normativas aplicables
- Colaborar en la gestión, implantación y control de los requisitos del Esquema Nacional de Seguridad (ENS)
- Informar sobre el desempeño del SGSI y las oportunidades de mejora

- Identificar y gestionar las acciones necesarias para el tratamiento de desviaciones detectadas en el SGSI y el ENS
- Informar al Comité de Seguridad de las actividades desarrolladas en el marco de las funciones de supervisión, gestión y coordinación que le han sido encomendadas
- Coordinar las tareas periódicas derivadas de la revisión y mantenimiento del análisis de riesgos
- Auxiliar al Comité de Seguridad en la elaboración, revisión y seguimiento periódico de las normativas generales de seguridad que derivan de esta política
- Elevar informes con planes de mejora basados en los resultados de las auditorías periódicas o cuando se encuentren deficiencias que supongan una amenaza para la seguridad de la información
- Comunicar al Comité de Seguridad el incumplimiento de la Política de Seguridad de la Información y de las normativas derivadas
- Redacción y presentación de propuestas al Comité de Seguridad

Este grupo de trabajo se reúne, al menos, cada dos meses, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

Las propuestas de decisión serán adoptadas por consenso de los miembros, que posteriormente deben trasladar al Comité de Seguridad para su aprobación final.

4.5. Directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso

ENS [org.1.5]

Para el desarrollo de la documentación de seguridad del sistema se establece un marco normativo estructurado en diferentes niveles, que permite complementar lo definido en el presente documento, así como definir y concretar las regulaciones y restricciones aplicables a los sistemas de información.

La normativa de seguridad se encuentra a disposición de todos los miembros de la organización que necesiten conocerla y, en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones a través de los repositorios documentales de AXIANS.

El criterio establecido es que cada colaborador debe tener siempre acceso a la Política de Seguridad de la Información y a toda la normativa que pueda ser relevante para el correcto desempeño de su trabajo.

Con carácter general, y en la medida de lo posible, se procura la integración de procesos para dar cumplimiento a exigencias de normativas diferentes, sin perjuicio de las particularidades específicas de cada ámbito.

El cuerpo normativo que desarrolla la PSI tiene los siguientes niveles:

- Primer nivel normativo: constituido por la presente Política, donde se establecen las directrices generales de seguridad aplicables y sirve de guía para la creación de normas de seguridad
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de la PSI, con el objetivo de establecer las pautas y directrices de los aspectos concretos del SGSI. Se determina qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los Sistemas de Información de la organización para así alcanzar los objetivos que persigue la presente política
- Tercer nivel normativo: constituido por los procedimientos, guías e instrucciones técnicas de Seguridad de la Información, en ellas se describe de forma concreta cómo proteger lo definido en las normas, identificando a los responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento

4.6. Gestión de Riesgos (riesgos y amenazas a la seguridad de la información)

ENS [op.pl.1] ; ISO27001 [6.1]

Para el análisis de riesgos, AXIANS emplea una herramienta de GRC corporativa, cuya metodología se encuentra alineada con la guía *ISO 31000 de Gestión del riesgo*, y se basa, en algunos aspectos, en metodologías internacionalmente reconocidas, por ejemplo, Magerit o el método William T. Fine.

De esta forma, la metodología de la herramienta persigue un doble objetivo:

- Estudiar los riesgos asociados a los sistemas de información y su entorno

- Recomendar las medidas necesarias para conocer, prevenir, impedir, reducir o controlar los riesgos estudiados

La herramienta está diseñada teniendo en cuenta los requisitos de los Sistemas de Gestión de Seguridad de la Información (ISO 27001/2), los requisitos de la normativa de privacidad (RGPD/LOPDGDD/ISO 27701) y del Esquema Nacional de Seguridad (ENS), lo que permite realizar evaluaciones de riesgos desde distintas perspectivas.

El nivel de riesgo se obtiene en base a la combinación de los datos de los activos, del catálogo de amenazas por categoría de activo, de la valoración de los niveles de Exposición y Probabilidad potencial (heredadas del contexto de riesgo de la organización), y la valoración del Impacto para cada una de las dimensiones evaluadas.

Dicha estimación se realiza de forma periódica, al menos una vez al año y, siempre que, se produzca un cambio en la información manejada, cuando cambien los servicios prestados, cuando ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

El propietario de un riesgo debe ser informado de los riesgos que afectan a los activos de su propiedad y del riesgo residual al que está sometido.

A la luz de los resultados del riesgo residual obtenido, y considerando los niveles de "apetito al riesgo" definidos en el Comité de Seguridad, se determina un conjunto de acciones orientadas a la reducción del riesgo residual hasta niveles aceptables. Las medidas acordadas se definen y documentan en la Declaración de Aplicabilidad vigente, y se mantiene evidencia de la revisión y aceptación de los riesgos residuales por parte de los propietarios del riesgo.

Todas las exenciones y excepciones previstas deben ser identificadas y descritas en la Declaración de Aplicabilidad, así como informar al Responsable de Seguridad de la Información. Dichas excepciones se analizan teniendo en cuenta los riesgos asociados, según su categorización, para determinar si pueden ser aceptadas o no.

4.7. Datos de carácter personal

ENS [mp.info.1] ; ISO27001 [A.5.34]

AXIANS cuando realiza tratamientos en los que se manejan datos de carácter personal, cumple con las medidas de seguridad de obligado cumplimiento que se establecen en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y la Ley Orgánica 3/2018,

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Además, cuenta con un Documento de Seguridad donde se desarrollan dichas medidas, que puede se encuentra publicado en la Intranet.

AXIANS solo trata los datos de carácter personal a los que tienen acceso en el desarrollo de sus funciones (empleados, candidatos y datos de contacto de clientes y proveedores). Solo tienen acceso a estos datos las personas autorizadas, a quienes se identifican y quienes cumplen con las medidas de seguridad establecidas para la protección de estos datos.

El desarrollo normativo de la presente política garantiza el cumplimiento por los responsables y encargados del tratamiento de los datos personales de los principios y obligaciones establecidas en el marco normativo de protección de datos con la participación adecuada y en tiempo oportuno, desde el diseño de los tratamientos y sus medios, al delegado de protección de datos, a través de las correspondientes medidas técnicas y organizativas, todo ello a través del marco organizativo de esta Política de Seguridad de la Información.

4.8. Terceras partes

ISO27001 [A.5.5] [A.5.6] [A.5.14]

Cuando AXIANS preste servicios o maneje información de terceras partes, se les hará partícipes de esta Política de Seguridad de la Información, y se establecerán canales comunicación y coordinación con otros Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando AXIANS utilice servicios o ceda información a terceros, se les hará igualmente partícipes de esta Política de Seguridad y de la Normativa de seguridad aplicable a dichos servicios o sistemas de información. Estas terceras partes quedarán sujetas a las obligaciones establecidas en dicha 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se realizará un informe por parte del Responsable de Seguridad de la Información, 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.

4.9. Obligaciones del personal

ENS [mp.per.2] [mp.per.3] [mp.per.4] ; ISO27001 [A.6.3]

Todos los colaboradores de AXIANS, tanto internos como externos, tienen la obligación de conocer y cumplir la presente Política de Seguridad de la Información y demás normativa de seguridad existente, siendo responsabilidad del Comité de Seguridad disponer de los medios necesarios para que la información llegue a los afectados.

Al menos una vez al año, se deben llevar a cabo acciones formativas, para formar y concienciar a los empleados en los aspectos más relevantes de los procedimientos de seguridad.

Las personas con responsabilidad en el uso, operación o administración de los sistemas deben recibir formación para el manejo seguro de los sistemas, en la medida en que la necesiten para realizar su trabajo.

En caso de incumplimiento de esta política, se derivarán sanciones de acuerdo con la legislación vigente, reglamento interno de AXIANS y contratos laborales, bajo la responsabilidad del departamento de Personas de AXIANS.

4.10. Cumplimiento de Políticas y Mejora Continua

ISO27001 [10.1] [A.5.35]

Para verificar que el Sistema de Gestión de la Seguridad de la Información es eficaz, y cumple con los requisitos que la normativa de seguridad establece, es necesario llevar a cabo auditorías planificadas y evaluaciones continuas de los procesos asociados, así como, auditorías extraordinarias, siempre que se produzcan modificaciones sustanciales en los sistemas de información y las operaciones en las que se sustentan los servicios, y que puedan repercutir en el cumplimiento de las medidas de seguridad requeridas, en los protocolos de actuación o en el aseguramiento de las operaciones. Se ha establecido, a nivel del Grupo Vinci Energies, la obligatoriedad de realizar 2 auditorías anuales de forma local en cada Polo, al menos a 2 unidades de negocio diferentes.

Por todo ello, es imprescindible la coordinación de los aspectos técnicos, jurídicos y organizativos de la compañía.

El resultado de dichas evaluaciones y auditorías deben identificarse como no conformidades, que son analizadas y tratadas a través de la definición de acciones correctivas apropiadas a los efectos de las no conformidades encontradas.

Adicionalmente, al seguimiento de no conformidades procedentes de evaluaciones y auditorías, existen otros aspectos que, mediante su revisión y seguimiento, contribuyen a alcanzar la mejora continua del SGSI, entre los que se encuentra:

- La Política de Seguridad de la Información
- La Categorización del Sistema
- El Análisis de Riesgos
- Los objetivos de Seguridad de la Información
- El análisis de eventos
- La Revisión por la Dirección

4.11. Aprobación y entrada en vigor

La presente política fue aprobada, en su anterior versión, el día 15 de marzo de 2022 por el Responsable de Seguridad de la Información y ha sido reemplazada por la presente versión, aprobada por la Dirección de AXIANS el 10 de octubre de 2024.

La Política de Seguridad de la Información se comunica a todas las partes interesadas a través de la página web de AXIANS. El Responsable de Seguridad Corporativa y el Responsable de Seguridad de la Información son responsables de mantener y revisar esta política, al menos una vez al año.

Dirección AXIANS

Versión 5.1

Fecha: 10/10/2024