

POL Política de seguridad de la información

Historial de versiones

Versión	Fecha	Autor	Aprobado por
1	18/03/2026	Carolina Figueroa Cuadros	Marc Delgado Olivella

Índice

- Propósito
- Campo de aplicación
- Referencias normativas
- Términos y definiciones
- Roles y responsabilidades
- Objetivos de seguridad de la información
- Principios fundamentales de seguridad de la información
- Protección de activos fuera de sede
- Archivado y actualización
- Documentos de referencia

Propósito

La Alta Dirección de SENSOTRAN, S.L.U. adopta la presente política como documento marco del Sistema de Gestión de la Seguridad de la Información (SGSI), con el fin de formalizar su compromiso con la protección de los activos informativos que sustentan la actividad de diseño, fabricación, comercialización, alquiler y mantenimiento de sistemas y equipos de detección y análisis de gases. Este documento establece el marco de referencia para instaurar, implementar, mantener y mejorar de forma continua el SGSI, de conformidad con el Esquema Nacional de Seguridad.

SENSOTRAN reconoce que la información constituye un activo estratégico cuya protección resulta esencial para preservar la confianza de sus clientes de los sectores químico, alimentario, energético, petroquímico, farmacéutico y medioambiental, así como para garantizar la continuidad de las operaciones desde su sede en El Prat de Llobregat (Barcelona). Mediante el SGSI, la organización promueve la salvaguarda de la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad de la información y de los servicios que presta, alineando los esfuerzos de seguridad con los objetivos estratégicos corporativos y con el marco jurídico y normativo aplicable.

La presente política impulsa un enfoque basado en el riesgo, la responsabilidad compartida y la mejora continua, principios que orientan el conjunto de políticas, procedimientos y normas de seguridad que conforman el SGSI.

Campo de aplicación

Esta política se aplica al sistema de información que da soporte a la actividad de diseño, fabricación, comercialización, alquiler y mantenimiento de sistemas y equipos de detección y análisis de gases de SENSOTRAN, S.L.U. Su alcance abarca la totalidad de procesos de negocio, activos informativos, infraestructuras tecnológicas y servicios, tanto propios como externalizados, desde la sede operativa ubicada en carrer Berguedà 1, planta 2, oficina A3, P. I. Mas Blau, Edificio Muntadas 1, 08820 El Prat de Llobregat (Barcelona). Involucra a todo el personal de la organización, incluyendo empleados, colaboradores, contratistas y terceras partes que accedan a la información o a los sistemas corporativos, con independencia de su ubicación.

Referencias normativas

- Real Decreto 311/2022
- Ley Orgánica 3/2018
- Reglamento (UE) 2016/679
- Ley 40/2015
- Ley 39/2015
- Ley 34/2002
- Real Decreto 4/2010

- CCN-STIC 801
- CCN-STIC 804
- CCN-STIC 817

Términos y definiciones

- **Confidencialidad** : propiedad de la información por la cual no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad** : propiedad de la información o de un activo consistente en ser exacta, completa y no haber sido alterada de forma no autorizada.
- **Disponibilidad** : propiedad de la información y los servicios de ser accesibles y utilizables a petición de una entidad autorizada.
- **Autenticidad** : propiedad que permite verificar la identidad de un sujeto o proceso, o el origen de los datos.
- **Trazabilidad** : propiedad que permite rastrear las acciones realizadas en un sistema de información hasta su origen o actor ejecutor.
- **Dimensión de seguridad** : cada uno de los aspectos de la información o del servicio objeto de valoración y protección, que comprende la disponibilidad, la autenticidad, la integridad, la confidencialidad y la trazabilidad.
- **Incidente de seguridad** : suceso inesperado o no deseado con consecuencias o probabilidad de afectar negativamente a la seguridad de un sistema de información o a los servicios que presta.

Roles y responsabilidades

- **Director General** : aprueba esta política, asigna los recursos necesarios para el SGSI y asume la responsabilidad última de la seguridad de la información en la organización.
- **Responsable del Sistema** : gestiona la documentación del SGSI, planifica la mejora continua y coordina la ejecución de auditorías internas.
- **Responsable Calidad Medio Ambiente** : garantiza la disponibilidad de recursos suficientes para implementar y mantener las medidas de seguridad establecidas en el marco del ENS.
- **Gestión de Proyectos** : vela por el cumplimiento de las obligaciones legales, contractuales y normativas aplicables en materia de seguridad de la información.
- Todo el personal, colaboradores y terceras partes: cumple las disposiciones de esta política, las normas y los procedimientos de seguridad del SGSI, y notifica de forma inmediata cualquier incidente, anomalía o debilidad de seguridad.

Funciones de seguridad en el marco del ENS

SENSOTRAN, en cumplimiento del principio de diferenciación de responsabilidades que establece el ENS, ha designado formalmente las siguientes funciones de seguridad, cuyo proceso de identificación, asignación y formalización se detalla en el *PRO Procedimiento de roles y responsabilidades* y en la *POL Política de roles y responsabilidades en materia de seguridad de la información*. La Alta Dirección aprueba cada nombramiento mediante acta formal, garantizando la segregación de funciones necesaria para el correcto ejercicio de cada responsabilidad.

Responsable de la Información

Determina los requisitos de seguridad de la información gestionada, estableciendo los niveles de seguridad en todas las dimensiones afectadas conforme al Anexo I del Real Decreto 311/2022. Aprueba formalmente dichos niveles, competencia no delegable, y actúa como propietario de los riesgos sobre la información, asumiendo el resultado residual del análisis y gestión de riesgos. Evalúa las consecuencias de un impacto negativo sobre la seguridad de la información, considerando los efectos sobre los objetivos de la organización, la protección de los activos, las obligaciones de servicio, la legalidad y los derechos de los ciudadanos. Mantiene actualizada la valoración ante cambios significativos en la naturaleza, el contexto o los riesgos de la información, y ostenta en todo momento la potestad exclusiva de modificar los niveles de seguridad asignados.

Responsable del Servicio

Establece los requisitos de seguridad de los servicios prestados, fijando los niveles de seguridad en las dimensiones pertinentes conforme al Anexo I del Real Decreto 311/2022. La aprobación formal de dichos niveles constituye una competencia igualmente no delegable. Define los servicios críticos para la organización y sus requisitos de seguridad asociados, e integra especificaciones de seguridad en el ciclo de vida de los servicios y sistemas. Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios y mantiene actualizada dicha valoración frente a cambios en la prestación o en los riesgos.

Responsable de Seguridad

Determina las medidas de seguridad aplicables a partir de las valoraciones realizadas por el **Responsable de la Información** y el **Responsable del Servicio**. Elabora y aprueba la *MOD Declaración de aplicabilidad (DoA) ENS*, determina la categoría del sistema y verifica que las medidas hayan sido implementadas adecuadamente. Participa en la elaboración de esta política y de los procedimientos del SGSI, promueve la formación y concienciación en seguridad de la información, analiza los riesgos asociados al despliegue de sistemas de inteligencia artificial y, ante incidentes de ciberseguridad, evalúa su gravedad y actúa como punto de contacto con las autoridades competentes.

Responsable del Sistema

Opera el sistema de información conforme a las medidas de seguridad establecidas, implementando la seguridad de forma concreta y supervisando las operaciones diarias. Define la topología del sistema, el marco de gestión, los criterios de uso y los servicios disponibles, así como la política de conexión y desconexión de equipos y nuevos usuarios. Aprueba los cambios que afecten a la seguridad operativa, determina la configuración autorizada de hardware y software y adopta las medidas correctoras derivadas de los informes de auditoría. Investiga los incidentes de seguridad que afecten al sistema e

informa al **Responsable de Seguridad** , y establece los planes de contingencia y continuidad para garantizar la disponibilidad del servicio.

Administrador del Sistema

Implementa, gestiona y mantiene las medidas de seguridad aplicables al sistema de información. Configura y actualiza el hardware y software que soportan los mecanismos de seguridad, elabora y aplica los procedimientos operativos de seguridad cuando así lo determine el **Responsable del Sistema** , e informa de cualquier anomalía o vulnerabilidad al **Responsable del Sistema** y al **Responsable de Seguridad** . Inicia el proceso de respuesta ante incidentes en el sistema bajo su responsabilidad y colabora en la definición de procedimientos de monitorización y en los planes de contingencia y emergencia.

La estructura organizativa general de SENSOTRAN se recoge en el *MOD Organigrama* , y las funciones y tareas asociadas a cada puesto se describen en el *MOD Manual de funciones* , asegurando que los deberes de seguridad estén integrados en las responsabilidades diarias de todo el personal.

Comité de Seguridad de la Información

SENSOTRAN ha constituido un Comité de Seguridad de la Información como órgano colegiado de gestión y coordinación de la seguridad. El Comité está integrado por el **Responsable de la Información** , el **Responsable del Servicio** , el **Responsable de Seguridad** , el **Responsable del Sistema** y el **Administrador del Sistema** ; adicionalmente, podrá convocar a otros colaboradores internos o externos cuando la materia lo requiera. Sus áreas de responsabilidad comprenden:

- Aprobar la política de seguridad de la información.
- Supervisar el cumplimiento del ENS.
- Aprobar las medidas de seguridad para los sistemas de información.
- Analizar y aprobar la gestión de riesgos.
- Revisar los incidentes de seguridad relevantes.
- Aprobar los planes de tratamiento de riesgos y de mejora.
- Supervisar las auditorías internas y externas.
- Aprobar los cambios significativos que puedan afectar a la seguridad de la información.
- Revisar periódicamente el estado del SGSI.

El Comité se reúne al menos una vez al año y, adicionalmente, ante la ocurrencia de un incidente grave de seguridad, ante cambios significativos en los sistemas de información o a solicitud de cualquiera de sus miembros. Las sesiones pueden celebrarse de forma presencial o por medios telemáticos, y de cada reunión se levanta acta.

Objetivos de seguridad de la información

SENSOTRAN persigue a través de su SGSI un conjunto de objetivos de seguridad estrechamente vinculados a su misión como proveedor de soluciones de detección y

análisis de gases y a las exigencias del ENS.

La organización se compromete a proteger la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad de la información gestionada y de los servicios prestados, adecuando las medidas de seguridad a la categoría del sistema y a los niveles determinados para cada dimensión en el *Informe sobre la clasificación y la evaluación del sistema*.

La gestión de riesgos constituye un pilar de la estrategia de seguridad. SENSOTRAN aborda de forma sistemática y proporcional los riesgos identificados, prestando atención prioritaria a aquellos con mayor impacto potencial; el análisis de riesgos y oportunidades vigente sitúa la ciberseguridad en nivel alto, por lo que la organización destina esfuerzos específicos a su mitigación, incluyendo la obtención de la certificación ENS.

El cumplimiento del marco jurídico y normativo aplicable representa otro objetivo esencial: SENSOTRAN garantiza que sus sistemas y servicios operen dentro de los límites definidos por el Real Decreto 311/2022, la Ley Orgánica 3/2018 y el Reglamento (UE) 2016/679, entre otras normas de referencia.

La continuidad de los servicios críticos que soportan las actividades de diseño, fabricación, comercialización, alquiler y mantenimiento de equipos de detección de gases ocupa un lugar central en la planificación de la seguridad, con el propósito de contener el impacto de los incidentes y ajustar los plazos de recuperación a las necesidades operativas.

SENSOTRAN fomenta una cultura de seguridad de la información entre todo su personal, reforzando la responsabilidad compartida mediante programas de formación y concienciación que abarquen tanto los aspectos técnicos como los organizativos y normativos.

La mejora continua del SGSI se sustenta en la revisión periódica de la eficacia de las medidas de seguridad, los resultados de las auditorías recogidos en el *MOD Informe de auditoría*, las conclusiones de la revisión por la dirección documentadas en el *MOD Acta de revisión de la dirección* y los indicadores de desempeño del sistema.

Principios fundamentales de seguridad de la información

SENSOTRAN articula su SGSI sobre los principios básicos que el ENS establece como fundamento de la seguridad de la información, proyectándolos en el día a día de la organización a través de sus políticas, normas y procedimientos.

La seguridad se concibe como un proceso integral que abarca todos los elementos humanos, materiales, técnicos, jurídicos y organizativos del sistema de información. Ninguna medida aislada resulta suficiente: es la combinación coordinada de controles de distinta naturaleza la que permite alcanzar niveles de protección proporcionados a la información y los servicios que la organización gestiona.

La toma de decisiones se fundamenta en la gestión de riesgos, de forma que la selección y el dimensionamiento de las medidas de protección respondan a la naturaleza de la información, a los servicios prestados y a los riesgos a los que están expuestos. SENSOTRAN mantiene un proceso estructurado de análisis y tratamiento de riesgos,

recogido en el *PRO Procedimiento de gestión de riesgos* , cuyas conclusiones alimentan la selección de medidas y la asignación de prioridades de actuación.

El enfoque de seguridad comprende cuatro fases indisociables: prevención, orientada a evitar la materialización de amenazas; detección, dirigida a descubrir anomalías e incidentes de forma oportuna; respuesta, encaminada a contener los incidentes y restablecer la normalidad operativa conforme al *PRO Procedimiento de gestión de incidentes de seguridad de la información* ; y recuperación, que garantiza la recuperación de datos y servicios con arreglo al *PRO Procedimiento de continuidad operativa y recuperación de emergencia* , así como la trazabilidad necesaria para la investigación posterior.

La protección del sistema se estructura en múltiples líneas de defensa, de modo que si una capa resulta insuficiente las restantes mitiguen el riesgo o ralenticen la amenaza. Esta defensa en profundidad combina controles físicos, definidos en el *PRO Procedimiento de seguridad física y ambiental* , con controles organizativos y lógicos que incluyen la segmentación de la red corporativa en zonas diferenciadas y una política de denegación por defecto del tráfico no autorizado.

La organización promueve la vigilancia continua de sus sistemas de información, supervisando de forma permanente su estado de seguridad para identificar oportunamente vulnerabilidades, eventos anómalos o modificaciones no autorizadas en la configuración. De manera complementaria, SENSOTRAN se compromete a reevaluar periódicamente las medidas de seguridad y la propia evaluación de riesgos, adaptando el SGSI a las variaciones del entorno, la aparición de nuevas ciberamenazas y la evolución tecnológica.

Clasificación y protección de la información

SENSOTRAN establece un sistema de clasificación de la información en tres niveles (confidencial, limitada y pública), detallado en la *POL Política de clasificación y etiquetado de la información* . Cada nivel lleva asociados requisitos de protección específicos para el tratamiento, la transmisión y la conservación de los datos, de modo que las medidas de seguridad resulten proporcionales a la sensibilidad de la información.

El **Responsable de la Información** determina y aprueba formalmente los niveles de seguridad de la información gestionada en las cinco dimensiones del ENS, documentando la valoración correspondiente. Cuando la información presenta restricciones en su tratamiento debido a su sensibilidad, se le asigna la clasificación adecuada y se aplican las medidas de protección exigidas para su nivel. El **Responsable de la Información** ostenta la potestad exclusiva de modificar los niveles de seguridad asignados, de conformidad con los criterios establecidos. Todo el personal autorizado para acceder a información clasificada se identifica y documenta en el *Registro de usuarios autorizados para el uso de la información* , y los tratamientos de datos personales se recogen en el *MOD Registro de tratamientos del responsable* .

La organización adopta la práctica de etiquetar la información clasificada como confidencial o limitada en todos los soportes, ya sean documentos electrónicos, correos electrónicos, medios físicos o contenidos multimedia, garantizando que su nivel de protección sea visible y reconocible en todo momento.

Protección del puesto de trabajo

SENSOTRAN promueve que los puestos de trabajo permanezcan despejados, sin material distinto del estrictamente necesario para la actividad en curso, y que una vez utilizado, todo material con información sensible se guarde en un lugar cerrado. Los documentos confidenciales en formato físico se custodian en ubicaciones de acceso controlado, de modo que la exposición no autorizada quede prevenida incluso cuando el puesto permanece temporalmente desatendido.

Esta práctica de escritorio limpio se complementa con la de pantalla limpia: la organización adopta el bloqueo automático de las sesiones de usuario tras un periodo razonable de inactividad, requiriendo una nueva autenticación para reanudar la actividad. La medida se aplica a todos los dispositivos corporativos, con independencia de que se encuentren en la sede o en situaciones de trabajo remoto.

Los parámetros técnicos concretos de bloqueo, las directrices de uso aceptable y la gestión de dispositivos se desarrollan en la *POL Política de seguridad operativa* y en el *PRO Procedimiento de gestión y control de accesos lógicos*.

Normas de uso y responsabilidad del personal

La organización establece normas de seguridad que regulan el uso correcto de los equipos, los servicios y las instalaciones, así como las conductas que se consideran uso indebido. Todo el personal asume la responsabilidad de cumplir estas normas, de proteger los activos informativos que utiliza en el desempeño de sus funciones y de notificar de forma inmediata cualquier incidente, debilidad o comportamiento anómalo que detecte.

El *Código de conducta* vincula la conducta ética del personal con la seguridad de la información, identificando comportamientos aceptables e inaceptables y definiendo las consecuencias disciplinarias por infracciones, que serán proporcionales a la gravedad de la falta, de conformidad con la legislación vigente. Los proveedores, colaboradores externos y consultores que gestionen información reservada formalizan su compromiso mediante la suscripción de un *MOD Acuerdo externo de no divulgación (NDA)*.

Estructura documental de seguridad

SENSOTRAN dispone de un conjunto estructurado de documentos que describen de forma clara y precisa cómo se utilizan los elementos del sistema de información, cómo se realizan las tareas habituales, quién es responsable de cada actividad, cómo se identifican y notifican los comportamientos anómalos y la forma en que la información se trata en función de su nivel de seguridad. Estos documentos abarcan, entre otros ámbitos, el control de accesos, el archivo, la copia, el etiquetado de soportes y la transmisión telemática.

La documentación del SGSI se organiza en políticas, procedimientos, instrucciones operativas y registros, cuyo inventario y estado de actualización se mantienen en la *MOD Lista de documentación*. La *MOD Matriz de servicios, sistemas, medidas de seguridad e información* vincula cada servicio y proceso de negocio con los sistemas de información que lo soportan y con los conjuntos de datos tratados. El marco normativo aplicable se recoge en la *MOD Lista de normas*, asegurando la trazabilidad entre los requisitos legales y las medidas de seguridad implementadas.

El acceso a la documentación de seguridad se restringe conforme al sistema de clasificación de la información, de modo que cada persona acceda únicamente a los documentos necesarios para el desempeño de sus funciones. Las políticas, procedimientos e instrucciones operativas del SGSI se comunican internamente a todo el personal y, cuando procede, se ponen a disposición de las partes interesadas externas.

Protección de activos fuera de sede

SENSOTRAN reconoce que sus activos informativos requieren protección también cuando se utilizan fuera de las instalaciones de la organización, en situaciones de trabajo remoto, desplazamiento profesional o colaboración con terceros. La organización se compromete a extender las medidas de seguridad a estos escenarios, de forma que la confidencialidad, la integridad y la disponibilidad de la información no se vean comprometidas por el cambio de entorno.

El personal que trabaje fuera de la sede utiliza exclusivamente dispositivos autorizados por la organización o expresamente aprobados conforme a las normas internas. La organización garantiza que los dispositivos portátiles incorporan medidas de protección proporcionadas a la sensibilidad de la información que gestionan, incluyendo mecanismos de cifrado, autenticación robusta y bloqueo automático por inactividad. Las conexiones remotas se realizan a través de canales seguros, y el espacio de trabajo se dispone de manera que personas no autorizadas no puedan visualizar la pantalla ni acceder a la documentación.

Los equipos corporativos no se dejan desatendidos en lugares públicos, vehículos ni zonas comunes de establecimientos. La organización fomenta la custodia responsable de todo activo fuera de la sede y la destrucción segura de la documentación confidencial en formato físico cuando deja de ser necesaria.

Cualquier incidente de seguridad relacionado con activos fuera de sede, incluidos el extravío, el robo o el deterioro de equipos, se notifica y gestiona conforme al *PRO Procedimiento de gestión de incidentes de seguridad de la información*, activándose las medidas de contención apropiadas. La *POL Política de seguridad operativa* desarrolla los controles específicos aplicables al trabajo remoto, la protección de dispositivos móviles y las comunicaciones seguras fuera de la sede.

Archivado y actualización

La presente política constituye un documento controlado del SGSI y se archiva en el repositorio documental de la organización conforme al sistema de gestión establecido. Su revisión se realiza con carácter al menos anual, o con anterioridad cuando se produzcan cambios significativos en la organización, en la tecnología, en el marco normativo o en el contexto de amenazas. El **Responsable del Sistema** coordina el proceso de revisión, y cualquier modificación requiere la aprobación del **Director General** y del Comité de Seguridad de la Información antes de su entrada en vigor.

Documentos de referencia

- PRO Procedimiento de roles y responsabilidades
- POL Política de roles y responsabilidades en materia de seguridad de la información
- PRO Procedimiento de gestión de riesgos
- PRO Procedimiento de gestión de incidentes de seguridad de la información
- PRO Procedimiento de continuidad operativa y recuperación de emergencia
- PRO Procedimiento de seguridad física y ambiental
- PRO Procedimiento de gestión y control de accesos lógicos
- POL Política de clasificación y etiquetado de la información
- POL Política de seguridad operativa
- Código de conducta
- Informe sobre la clasificación y la evaluación del sistema
- MOD Declaración de aplicabilidad (DoA) ENS
- MOD Organigrama
- MOD Manual de funciones
- MOD Lista de documentación
- MOD Lista de normas
- MOD Matriz de servicios, sistemas, medidas de seguridad e información
- MOD Registro de tratamientos del responsable
- MOD Acuerdo externo de no divulgación (NDA)
- MOD Informe de auditoría
- MOD Acta de revisión de la dirección
- Registro de usuarios autorizados para el uso de la información

POL Política del sistema de gestión

Historial de versiones

Versión	Fecha	Autor	Aprobado por
1	18/03/2026	Carolina Figueroa Cuadros	Marc Delgado Olivella

Índice

- Propósito
- Campo de aplicación
- Referencias normativas
- Términos y definiciones
- Roles y responsabilidades
- Compromiso y objetivos del sistema de gestión
- Archivado y actualización
- Documentos de referencia

Propósito

SENSOTRAN SLU reconoce que la seguridad de la información constituye un pilar estratégico para el desempeño sostenible de sus actividades de diseño, fabricación, comercialización, alquiler y mantenimiento de sistemas y equipos de detección y análisis de gases. La presente política establece el compromiso de la Alta Dirección con la protección de los activos de información y los servicios que la organización presta, en consonancia con las exigencias del Esquema Nacional de Seguridad y el marco regulatorio aplicable en materia de protección de datos y seguridad.

A través de este documento, SENSOTRAN promueve un entorno en el que la seguridad se concibe como un proceso integral que abarca dimensiones humanas, técnicas, organizativas y legales. La organización impulsa una cultura de responsabilidad compartida para que cada persona que interviene en la operativa empresarial comprenda su contribución a la protección de la información y actúe conforme a los principios aquí establecidos, los cuales se desarrollan en detalle en la *POL Política de seguridad de la información* y en el conjunto de documentos que conforman el cuerpo normativo del SGSI.

Campo de aplicación

La presente política se aplica al sistema de información que da soporte a la actividad de SENSOTRAN SLU desde su sede operativa en carrer Berguedà 1, planta 2, oficina A3, P.I. Mas Blau, 08820 El Prat de Llobregat (Barcelona). Comprende la totalidad de los procesos de negocio, los activos de información, las infraestructuras tecnológicas y los servicios tanto internos como externalizados. Vincula a todo el personal, colaboradores, contratistas y terceros que accedan a información o sistemas corporativos, con independencia de su ubicación física. El sistema de información se encuentra clasificado en categoría MEDIA conforme al *Informe sobre la clasificación y la evaluación del sistema* y al Anexo I del Real Decreto 311/2022. Quedan excluidos aquellos procesos que no interactúan directamente con los activos de información ni con los servicios amparados por el Sistema de Gestión de la Seguridad de la Información (SGSI).

Referencias normativas

- Real Decreto 311/2022
- Reglamento (UE) 2016/679
- Ley Orgánica 3/2018

Términos y definiciones

- **Sistema de información** : conjunto organizado de recursos destinados a la recogida, almacenamiento, procesamiento y transmisión de información.
- **Seguridad de la información** : protección de la información y los servicios frente a amenazas y vulnerabilidades que puedan afectar a su disponibilidad, confidencialidad,

integridad, autenticidad o trazabilidad.

- **Categoría de seguridad** : clasificación del sistema de información en función del impacto que tendría un incidente de seguridad sobre los servicios prestados y la información tratada.
- **Análisis de riesgos** : proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.
- **Disponibilidad** : propiedad de la información y los servicios de ser accesibles y utilizables cuando lo requiera una entidad autorizada.
- **Confidencialidad** : propiedad de la información de no ser puesta a disposición o revelada a individuos, entidades o procesos no autorizados.
- **Integridad** : propiedad de la información de ser exacta y completa.
- **Autenticidad** : propiedad consistente en que una entidad es quien dice ser o que garantiza la fuente de la que proceden los datos.
- **Trazabilidad** : propiedad consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Roles y responsabilidades

Director General / Responsable del Sistema: aprueba formalmente la política de seguridad, valida las decisiones estratégicas en materia de seguridad, autoriza la asignación de los recursos necesarios para el SGSI, aprueba el umbral de tolerancia al riesgo y resuelve las discrepancias del Comité de Seguridad de la Información.

Gerencia / Responsable de la Seguridad y del Servicio: elabora y actualiza el borrador de la política, incorporando las medidas de seguridad aplicables y la Declaración de Aplicabilidad vigente.

Responsable del Sistema de Gestión: recopila los elementos de entrada para la revisión de la política, archiva las versiones aprobadas, coordina su difusión interna y gestiona su publicación externa.

Gestión de Proyectos / Responsable de la Información: determina los requisitos de seguridad de la información gestionada, aprueba formalmente los niveles de seguridad asignados a los activos esenciales y acepta el riesgo residual.

Responsable Calidad Medio Ambiente: verifica la disponibilidad de recursos suficientes para implementar y mantener las medidas de seguridad establecidas en el marco del Esquema Nacional de Seguridad.

Compromiso y objetivos del sistema de gestión

Compromiso de la Alta Dirección

SENSOTRAN SLU, a través de su Alta Dirección, asume la responsabilidad última sobre la protección de los activos de información y la continuidad de los servicios que la

organización presta a sus clientes en los sectores químico, alimentario, energético, petroquímico, farmacéutico y medioambiental. El **Director General** respalda esta política como expresión de la voluntad corporativa de mantener un SGSI adecuado al contexto, a la actividad de la empresa y a sus orientaciones estratégicas.

La organización se compromete a:

- Cumplir los requisitos legales y reglamentarios aplicables a la seguridad de la información, en particular el Real Decreto 311/2022, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, así como cualesquiera obligaciones contractuales derivadas de la relación con sus clientes y proveedores.
- Proporcionar los recursos financieros, humanos y tecnológicos necesarios para implantar, mantener y mejorar de forma continua el SGSI, asegurando que las medidas de seguridad sean proporcionales a la categoría MEDIA del sistema de información.
- Impulsar la mejora continua del SGSI mediante revisiones periódicas, auditorías, indicadores de rendimiento y acciones correctivas que refuercen progresivamente la postura de seguridad de la organización.
- Fomentar una cultura de seguridad compartida en la que la sensibilización y la formación constituyan herramientas permanentes para que todo el personal comprenda y asuma sus responsabilidades en la protección de la información.

Principios rectores

La actividad de seguridad de la información en SENSOTRAN se sustenta en los principios que rigen el Esquema Nacional de Seguridad y que orientan todas las decisiones, inversiones y actuaciones en esta materia:

- **Seguridad como proceso integral** : la protección de la información no se limita a medidas técnicas aisladas, sino que integra elementos humanos, materiales, técnicos, jurídicos y organizativos, configurando un enfoque holístico que involucra a toda la organización.
- **Gestión basada en riesgos** : las decisiones de seguridad se fundamentan en un análisis sistemático y proporcionado, que identifica las amenazas y vulnerabilidades relevantes para los activos esenciales y calibra las medidas de protección en función del impacto potencial, de conformidad con las directrices contenidas en *PRO Procedimiento de gestión de riesgos* .
- **Prevención, detección, respuesta y recuperación** : la organización adopta un ciclo de seguridad en cuatro fases que permite anticiparse a las amenazas, identificar oportunamente los incidentes, contener sus efectos y restablecer la normalidad operativa en el menor tiempo posible.
- **Defensa en profundidad** : la protección se articula en múltiples capas de controles complementarios, de modo que el fallo de una medida individual no comprometa la seguridad global del sistema.
- **Vigilancia continua** : los controles de seguridad se someten a supervisión y reevaluación periódicas, garantizando su adecuación frente a la evolución del contexto tecnológico, normativo y de amenazas.

Objetivos estratégicos de seguridad

La Alta Dirección establece los siguientes objetivos estratégicos, que constituyen el marco de referencia para la planificación y evaluación del SGSI:

1. Proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y los servicios, calibrando las medidas de seguridad conforme a la categoría MEDIA del sistema de información.
2. Gestionar los riesgos de forma sistemática y proporcionada, prestando especial atención a los riesgos de ciberseguridad, y manteniendo el nivel de riesgo residual dentro del umbral de tolerancia aprobado por el **Director General** y aceptado formalmente por la **Responsable de la Información**.
3. Garantizar el cumplimiento del marco legal y reglamentario aplicable, incluidos el Real Decreto 311/2022, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.
4. Asegurar la continuidad de los servicios críticos que dan soporte a las actividades de detección y análisis de gases, minimizando el impacto de posibles interrupciones sobre la operativa y los compromisos con los clientes.
5. Promover una cultura de seguridad compartida mediante programas de formación y concienciación dirigidos a todo el personal, colaboradores y terceros con acceso al sistema de información.
6. Impulsar la mejora continua del SGSI a través de revisiones por la dirección, auditorías internas, indicadores de desempeño y acciones correctivas, conforme a lo previsto en *PRO Gestión de revisión por la dirección* y *PRO Procedimiento de mediciones y monitoreo*.

Cada objetivo se concreta en indicadores medibles, metas cuantificables, plazos de cumplimiento y responsables asignados, cuyo seguimiento se realiza de acuerdo con lo establecido en *PRO Procedimiento de mediciones y monitoreo*. recogidos en el MOD Indicadores del sistema de gestión, cuyo seguimiento se realiza de acuerdo con lo establecido en *PRO Procedimiento de mediciones y monitoreo*.

Comunicación y disponibilidad de la política

SENSOTRAN reconoce que la eficacia de esta política depende de su conocimiento por todas las personas a las que afecta. La organización se compromete a difundir la política entre todo el personal y las partes interesadas internas, destacando las modificaciones relevantes en cada actualización. Asimismo, la mantiene accesible para las partes interesadas externas a través del sitio web corporativo, de conformidad con los requisitos de disponibilidad previstos en el Esquema Nacional de Seguridad. Las modalidades específicas de comunicación y distribución se detallan en *PRO Procesos directivos*.

Archivado y actualización

La presente política se conserva como información documentada controlada dentro del SGSI. El **Responsable del Sistema** archiva cada versión aprobada, retira las versiones anteriores y mantiene la trazabilidad del historial de revisiones. La revisión se lleva a cabo

al menos una vez al año, coincidiendo con el ciclo de revisión por la dirección, o de forma extraordinaria cuando se produzcan cambios significativos en el contexto organizativo, en el marco normativo o tras un incidente de seguridad grave. Toda modificación requiere la aprobación formal del **Director General** antes de su entrada en vigor.

Documentos de referencia

- POL Política de seguridad de la información
- PRO Procesos directivos
- PRO Procedimiento de gestión de riesgos
- PRO Gestión de revisión por la dirección
- PRO Procedimiento de mediciones y monitoreo
- Informe sobre la clasificación y la evaluación del sistema