
# Política de Seguridad de la Información

Esquema Nacional De Seguridad

**Versión:** 0

**Fecha de aprobación:** 10/12/2025

**Estado:** Aprobada

**Control de cambios**

| Versión | Fecha | Elaborada por | Revisada por | Aprobada por | Motivo del cambio |
|---|---|---|---|---|---|
| 0 | 10/12/2025 | CDE | Comité Seguridad | Fernando Asenjo | Edición inicial |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Documentos de referencia**

- Esquema Nacional del Seguridad
- Norma ISO 27001
- Norma ISO 27002

**Nivel de seguridad:**

| | |
|---|---|
| General | ☒ |
| Restringido | |
| Confidencial | |

Contenido

## 1. Introducción

La Política de Seguridad de la Información (PSI) establece el conjunto de principios básicos y líneas de actuación de **Trebide** en relación a la seguridad de la información de sus servicios.

El objetivo de la seguridad es proteger los sistemas, la información y la continuidad a través de una actuación preventiva que minimice los riesgos, del seguimiento de la actividad diaria y de la rapidez de reacción ante incidentes.

**Trebide** es una compañía de servicios tecnológicos especializada en la aplicación de la tecnología para la operación de tecnologías de transporte y securización de infraestructuras críticas.

Prestamos servicios de ingeniería, integración y desarrollo tecnológicos para una óptima adecuación de las soluciones tecnológicas a los procesos de nuestros clientes. Combinamos nuestra dilatada experiencia sectorial junto con nuestras capacidades tecnológicas para hacer que nuestros clientes evoluciones sus negocios utilizando todo el potencial de la tecnología, adaptándola a sus necesidades actuales y futuras.

## 2. Marco Normativo

El marco normativo para la prestación de los servicios es el siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- 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 y por el que se deroga la Directiva 95/46/CE.
- 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 Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- Guías CCN-STIC:
    - 802 auditoria del ENS.
    - 807 criptología de empleo en el ENS.
    - 808 verificación del cumplimiento de las medidas en el ENS.
    - 809 declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento.
    - 825 Esquema Nacional de Seguridad. Certificaciones 27001.
- Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas) y de Auditoría de la Seguridad de los Sistemas de Información (Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública).
- UNE - ISO/IEC 27002 Código de buenas prácticas para la Gestión de la Seguridad de la Información.

- UNE - ISO/IEC 27001 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.

## 3. Alcance

Esta Política de Seguridad de la Información (PSI) establece el marco general para la gestión de la seguridad de la información en **Trebide**, una entidad del sector privado dedicada al desarrollo y la gestión operativa de herramientas y soluciones TIC (software y plataformas) para la gestión de seguridad física y lógica. Dado que nuestros servicios son prestados habitualmente a entidades del Sector Público español, esta PSI es plenamente conforme al Esquema Nacional de Seguridad (ENS), según lo dispuesto en el Artículo 2 del Real Decreto 311/2022.

El alcance de esta política abarca todos los sistemas de información, activos, procesos, personal y ubicaciones que gestionan, procesan o almacenan información de la organización o de sus clientes.

De cualquier modo, aunque esta PSI inspirada en el ENS será de aplicación a la totalidad de los procesos de la organización, ello no debe interpretarse como un compromiso de la organización por garantizar que todas esas áreas cumplen el ENS en una categoría determinada. Los sistemas de información que habrán de cumplir y obtener un certificado de adecuación al ENS serán aquellos expresamente designados por la organización en cada caso.

Los sistemas de información que deberán adecuarse al ENS se recogen en el Anexo I de esta Política.

## 4. Compromiso con la Seguridad

**Trebide** es consciente de la relevancia que tiene la información en el desarrollo de sus actividades y la considera un activo crítico de la compañía. De este modo velar por la seguridad de la información es una obligación que debe garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información crítica.

Para ello es necesario identificar las áreas en las que se deben concentrar los esfuerzos y desarrollar e implementar un sistema de gestión que proteja los recursos de información, servicios y productos frente a posibles amenazas. Los aspectos fundamentales a los que responden los objetivos del sistema son los siguientes:

- La actividad de **Trebide** genera de forma continua propiedad intelectual tanto como bien propio como bien de terceros. Para ello hace uso de recursos propios, recursos externos o ambos al mismo tiempo. La protección de toda propiedad intelectual debe ser una máxima en todos los procesos involucrados en su creación.
- La orientación al cliente implica el continuo intercambio de información y datos, originada tanto por el cliente como por **Trebide**. Esta información está estrechamente relacionada con el negocio de ambos y en muchas ocasiones puede ser sensible. Por este motivo y con objeto de ofrecer un buen servicio al cliente, **Trebide** debe garantizar de forma responsable la protección, en todas sus dimensiones, de la información de sus clientes en todos los procesos y servicios ofrecidos.
- **Trebide** es una empresa internacional donde el carácter multilateral es un valor diferencial con el resto de los competidores. Facilitar el intercambio de información y compartirla es un hecho inherente a la actividad que debe ser protegido y asegurado para garantizar el éxito del modelo.

- El carácter internacional y multilocal de **Trebide** proporciona un escenario de movilidad geográfica que afecta al uso y transporte de la información en itinerancia, tanto de uso propio como de uso compartido. Es nuestra responsabilidad garantizar la seguridad de esta información en itinerancia facilitando y contribuyendo al uso de recursos y de la información para todo el personal de **Trebide** susceptible de desarrollar sus funciones en un contexto de movilidad geográfica.

El sistema de gestión de Seguridad de la Información nos asegura un nivel de seguridad óptimo en nuestros procesos a través de la prevención de los fallos de seguridad, la potenciación de la mejora continua en todos nuestros procesos y el cumplimiento de los requisitos tanto legales como contractuales e internos.

## 5. Principios

Los principios en los que **Trebide** basa su sistema de Seguridad de la Información son los siguientes:

- **Seguridad como proceso integral:** La Dirección de **Trebide** se compromete con la Seguridad de la Información y la tiene en cuenta para que sea coordinada e integrada en la estrategia global. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información
- **Diferenciación de responsabilidades:** Que identifica las responsabilidades de todas las personas que participan en el servicio. Siempre se identifica a las personas responsables de la información (que determina los requisitos de Seguridad de la Información que se trata), del servicio (que determina los requisitos de seguridad de los servicios y productos), del sistema (que tiene la responsabilidad sobre la prestación de los servicios) y de la seguridad (que determina las decisiones para satisfacer los requisitos de seguridad).
- **Prevención, detección, respuesta y conservación:** en el que se gestionan y controlan todos los elementos técnicos, humanos, materiales y organizativos para que la Seguridad de la Información sea parte integral de la actividad habitual. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta
- **Gestión de los riesgos:** identificando y valorando las amenazas para establecer acciones de minimización del riesgo a niveles aceptables. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.
- **Existencia de líneas de defensa:** El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.
- **Vigilancia continua y reevaluación periódica:** a través del seguimiento del desempeño del sistema y el establecimiento de mejoras que aumenten la eficacia del sistema. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

## 6. Misión y objetivos

La misión y los objetivos de seguridad de **Trebide** se centran en:

- Garantizar en todo momento la seguridad y protección de la información.
- Motivar y concienciar a personas y usuarios/as respecto a la Seguridad de la Información.
- Control de los activos.
- Garantizar la seguridad física, protegiendo los activos de amenazas físicas y ambientales y emplazándolos en áreas seguridad con control de acceso.
- Garantizar la seguridad en la gestión de comunicaciones y operaciones.
- Control de acceso eficaz a los activos de información.
- Garantía de seguridad en todas las fases del ciclo de vida de los servicios.
- Detección y gestión 100% de los incidentes.
- Garantía de prestación continuada del servicio.
- Protección de datos de carácter personal.
- Cumplimiento de todos los requisitos legales y contractuales en materia de seguridad.

### a. Prevención

La seguridad debe ser una parte integral de cada una de las etapas del ciclo de vida de los sistemas, para ello se deben aplicar las medidas de seguridad requeridas por el ENS.

En las ofertas y licitaciones deben identificarse y ser tenidos en cuenta los requisitos de seguridad.

Para garantizar el cumplimiento de la política de prevención se debe:

- Revisar el sistema periódicamente.
- Autorizar los sistemas antes de su puesta en servicio.

### b. Detección

La detección de los incidentes que pueden degradar el sistema se realiza a través de la monitorización continuada.

### c. Respuesta

Se establecen los métodos para responder a los incidentes de seguridad.

### d. Recuperación

La disponibilidad de los servicios críticos se garantiza a través de los planes de continuidad de los sistemas que forman parte del plan de continuidad de negocio.

## 7. Organización de la seguridad

Además de las responsabilidades que se describen en los procesos, procedimientos, instrucciones y resto de documentación del sistema, se refieren a continuación las responsabilidades y tareas específicas de los diferentes puestos en relación al sistema de Seguridad de la Información.

Se establece que los propietarios de los procesos son a su vez los propietarios de los activos con los que se relacionan, salvo para los activos que se comparten con diferentes procesos en cuyo caso el propietario del activo es el servicio de TI y los activos que se relacionan con seguridad física y equipamiento auxiliar cuya propiedad es de Servicios Generales.

Además de las responsabilidades relativas a la gestión de la seguridad de la información en la organización en su conjunto, para aquellos sistemas que se hayan determinado como sometidos al

ENS por la Dirección, se designarán cuatro roles específicos, que se detallan a continuación. La designación formal de tales personas se acompaña al presente documento como Anexo II.

## a. Responsabilidades y perfiles generales

### i. Dirección del Negocio

La dirección del negocio tiene la responsabilidad y autoridad para:

- Asegurar que el sistema de gestión de la información es conforme con los requisitos
- Aprobación de Políticas de Seguridad.
- Identificación de requisitos y objetivos de negocio.
- Asignación de recursos.
- Formación y concienciación del personal.
- Revisión del sistema de gestión de la Seguridad de la Información.

### ii. Comité De Seguridad

El Comité de Seguridad debe asegurar, entre otras, la implantación de las normativas y procedimientos para la gestión de la Seguridad de la Información dentro de **Trebide** mediante el compromiso y la asignación de recursos adecuados.

- Máximo órgano de gestión de la seguridad dentro de **Trebide**.
- Es el órgano responsable de proporcionar las directrices de gestión de la Seguridad de la Información en cada centro, garantizando una dirección clara y un apoyo visible por parte de la Dirección a las iniciativas de seguridad, aprobando y realizando un seguimiento continuo de las acciones realizadas en materia de Seguridad de la Información.
- Debe asegurar entre otras la implantación de las normativas y procedimientos del Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de la organización mediante el compromiso y la asignación de recursos adecuados.
- Creación, mantenimiento y actualización de las Políticas de Seguridad.
- Asignación de Roles y Responsabilidades principales en materia de seguridad.
- Asegurar la implantación de los controles para la adquisición, tratamiento, almacenamiento y distribución de la información.
- Establecimiento de mecanismos de recolección y custodia válidos de evidencias.
- Establecimiento de medidas preventivas / correctoras ante desviaciones detectadas en las revisiones periódicas de los elementos que componen el SGSI.
- Establecimiento de medidas preventivas / correctoras ante desviaciones detectadas en las revisiones periódicas de cumplimiento en materia de protección de datos de carácter personal.
- Establecimiento de medidas preventivas / correctoras ante desviaciones detectadas en cualquier otro tipo de revisión (de seguridad) efectuada.
- Acordar y establecer metodologías y métricas estándares para la Gestión de la Seguridad de la Información.
- Planificar y diseñar las acciones de formación y concienciación específicas en materia de Seguridad de la Información y de protección de datos de carácter personal.

El Comité de Seguridad estará compuesto por la Dirección de la organización, el Coordinador del SGSI y los responsables específicos de aquellos sistemas que la organización haya designado como requeridos para el cumplimiento del ENS.

### iii. Coordinador del SGSI

- 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 TIC.
- Participar 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 de los sistemas.
- Gestionar los procesos de certificación.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia del Comité) y poner en conocimiento al Comité de las modificaciones que se hayan realizado a lo largo del periodo en curso.

## b. Responsabilidades y perfiles específicos para los sistemas alineados con el ENS

### iv. Responsable de la Seguridad

- Determinación de la categoría del sistema
- Realización del análisis de riesgos
- Elaboración de la Declaración de aplicabilidad
- Determinación de las medidas de seguridad adicionales que puedan ser necesarias.
- Definición de la configuración de seguridad del sistema.
- Elaboración de la documentación de seguridad del sistema.
- Elaboración de la normativa de seguridad del Sistema.
- Aprobación de los procedimientos de seguridad del sistema.
- Reportar, al comité de Seguridad, el estado de la seguridad del sistema.
- Aprobar el ciclo de vida del sistema: especificación, arquitectura, desarrollo, operación, cambios.

### v. Responsable del Sistema

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- 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 la Seguridad, el Coordinador del SGSI y/o Comité de Seguridad de la Información de la Información.
- Participar 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, en su caso, 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.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

### vi. Responsable del Servicio

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Describe los requisitos de Desarrollo.
- Vela por el cumplimiento de las metodologías de desarrollo, así como de los requisitos de seguridad del producto.
- Junto al Responsable de la Información, determinar los niveles de seguridad requeridos en cada dimensión .
- Establecer los requisitos del servicio en materia de seguridad.
- Junto al Responsable de la Información, aceptar el riesgo residual.

En los casos en los sistemas de información sometidos al ENS den soporte a un servicio prestado a terceros, particularmente Administraciones Públicas, los requisitos de la información pueden venir determinados por dichos terceros, precisamente en el marco del contrato de prestación de servicios que corresponda. En cualquier caso, a fin garantizar un marco de gobernanza estable y claro, la organización designará internamente a un Responsable del Servicio para dichos sistemas, cuyo papel consistirá en validar tales requisitos y hacerlos llegar a las personas correspondientes a fin de garantizar su cumplimiento.

### vii. Responsable de la Información

- Establece los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación sobre protección de datos.
- Determina los niveles de Seguridad de la Información.

En los casos en los sistemas de información sometidos al ENS den soporte a un servicio prestado a terceros, particularmente Administraciones Públicas, los requisitos de la información pueden venir

determinados por dichos terceros, precisamente en el marco del contrato de prestación de servicios que corresponda. En cualquier caso, a fin garantizar un marco de gobernanza estable y claro, la organización designará internamente a un Responsable de la Información para dichos sistemas, cuyo papel consistirá en validar tales requisitos y hacerlos llegar a las personas correspondientes a fin de garantizar su cumplimiento.

### c. Procedimiento de designación

El Coordinador del SGSI será designado por la Dirección. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Los responsables de la Información y el Servicio, en el caso de los sistemas sometidos a ENS, serán designados por la Dirección, por el tiempo que se determine en cada caso.

El Responsable de Seguridad del Sistema será nombrado por la dirección a propuesta del Comité de Seguridad, por el tiempo que se determine en cada caso.

## 8. Estructura de la documentación

El Coordinador del SGSI es quien se responsabiliza del control de la documentación del sistema, la documentación del mismo se divide en:

- Política de Seguridad.
- Políticas y normas específicas.
- Procedimientos e instrucciones.

Para los sistemas de información designados como sometidos al ENS por la Dirección, el Responsable de la Seguridad correspondiente elaborará la documentación de seguridad específica de tales sistemas, cumpliendo con los requisitos aplicables del ENS.

## 9. Datos de carácter personal

Trebide garantiza la protección de los datos de carácter personal tratados en el desarrollo de sus actividades, cumpliendo con lo establecido en el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD).

Se aplican medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad acorde al riesgo, incluyendo:

- Cifrado de datos personales.
- Control de accesos basado en el principio de mínimo privilegio.
- Registro de actividades de tratamiento.
- Evaluaciones de impacto cuando proceda.
- Formación específica en protección de datos para el personal con acceso a información personal.
- Procedimientos para el ejercicio de derechos por parte de los interesados.

El responsable de la protección de los datos personales es el Delegado de Protección de Datos (DPO) de Trebide, quien vela por el cumplimiento de la normativa vigente, asesora a la organización en materia de privacidad y actúa como punto de contacto con la Agencia Española de Protección de Datos (AEPD) y con los interesados.

## 10. Gestión de riesgos

El sistema de Seguridad y los productos y servicios se sustentan sobre un análisis de riesgos en el que se evalúan las amenazas y riesgos a los que está expuesto. El análisis se realiza:

- Anualmente.
- Cuando se produzcan cambios significativos en los productos y/o servicios
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad 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.

## 11.Responsabilidades del personal

Todas las personas que se relacionen con el ciclo de vida del servicio cumplirán con las políticas, normas y procedimientos establecidos.

Se realizarán sesiones de concienciación periódicas.

Las personas con responsabilidad en el uso, operación o administración de productos y /o servicios recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

## 12.Terceras partes

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información.

Dicha tercera parte quedará sujeta 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 requerirá un informe del Responsable de Seguridad 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.