POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN - POLÍTICAS

Fecha: 18/06/2025

Nº de versión: 5.0

Control de versiones

VERSIÓN	RESPONSABLE	DESCRIPCIÓN	FECHA
1.0	Pedro Miranda	Versión inicial	20/05/2022
2.0	Luis Santos	Revisión y ampliación contenidos	18/04/2023
3.0	Luis Santos	Revisión contenidos	25/04/2024
4.0	Luis Santos	Revisión y cambio formato + índices	29/05/2025
5.0	Luis Santos	Cambios menores y correcciones	18/06/2025

Contenido

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Propósito

Conscientes de la necesidad de contar con Sistemas Normalizados de reconocimiento internacional, la organización ha alineado su Sistema de Gestión de la Seguridad de la Información (SGSI) a los requisitos de los referenciales **UNE-EN ISO/IEC 27001:2022** y **del ESQUEMA NACIONAL DE SEGURIDAD Español (ENS nivel medio)**.

2. Alcance de la política

Los Sistemas de Información que dan soporte a las infraestructuras, los servicios y la seguridad aplicados a:

a) Instalación y mantenimiento de equipos y redes de comunicación.
b) Instalación y mantenimiento de energía renovable solar y estaciones de recarga de vehículos eléctricos.
c) Instalación de equipos de seguridad.
d) Prestación de los servicios de gestión y supervisión de las empresas del grupo.
e) Consultoría tecnológica, soporte y servicios gestionados.

Según declaración de aplicación en vigor a la fecha de emisión del certificado.

3. Declaración de compromiso

La Dirección se compromete a liderar y mantener un **Sistema de Gestión de Seguridad de la Información** en la organización basado en la **mejora continua** y en los siguientes **objetivos generales**:

- El serio compromiso de conocer las necesidades y expectativas de nuestros clientes y partes interesadas, para lograr su satisfacción, y de mejora continua, estableciendo y verificando el cumplimiento de los objetivos y metas anuales.
- El compromiso del cumplimiento de la legislación y reglamentación aplicable, así como de los requisitos que se suscriban.
- Asegurar la seguridad de la información propia y de nuestros clientes. Nuestra actividad implica el tratamiento de información variada como forma de ejecutar procesos básicos propios de su actividad. Sabiendo que los sistemas de información, aplicaciones, infraestructuras de comunicaciones, archivos y bases de datos, constituyen un activo importante de la empresa, la dirección prioriza la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información a la hora de definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas y vigila el cumplimiento del marco legal, de las directivas y políticas específicas y de los procedimientos definidos.
- El compromiso por la revisión continua de las competencias y mejora continua, a fin de garantizar la calidad de los servicios y su capacidad de afrontar los retos crecientes que nos plantean nuestros clientes.
- Desarrollo y disposición general de una estructura documental eficaz para la gestión del Sistema de Información, basados en:
  - Directrices y políticas de Seguridad de la Información y procedimientos generales operativos.
  - Marco normativo de seguridad.
  - Listado de documentos (internos y externos) del sistema para el control de versiones y vigencia.

4. Principios generales

ZENER utiliza los sistemas TIC (Tecnologías de la información y comunicación) para la prestación de sus servicios y el desempeño de sus procesos, que deben ser administrados y regulados con la aplicación de medidas que garanticen su protección, frente a daños intencionados o de carácter accidental, que pudieran impactar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información que gestionan, teniendo en cuenta que la Organización utiliza la clasificación de uso no restringido para la considerada como pública, así como las categorías uso restringido y

confidencial para los datos personales, sensibles e información operacional, indicando su adecuado manejo según lo establecido en el SGSI.

Por tanto, la misión de esta Política es garantizar la calidad de la información, su disponibilidad, así como la de los activos y servicios que la sustentan, para proporcionar su uso confiable y seguro a nuestros clientes, empleando para ello técnicas preventivas, seguimiento sobre la práctica diaria, y la identificación de incidentes con su adecuada respuesta.

La colaboración de las diferentes áreas de negocio interno, avala la repuesta ante la posible materialización de amenazas, las cuáles, trabajan conforme a las directrices que son desplegadas desde el Sistema de Gestión de Seguridad de la Información, y el Esquema Nacional de Seguridad que engloban, buenas prácticas de seguridad lógica y física, las relacionadas con el manejo de datos e información, así como vías de comunicación para incidencias, junto con la batería de medidas técnicas que corresponden al mantenimiento de Infraestructuras y Servicios TI internos.

Así pues, se constituyen procesos que permiten la **prevención y detección de incidentes de seguridad**, y la posterior **recuperación** conforme al acuerdo del Artículo 7 del Esquema Nacional de Seguridad, especificados como:

- **Prevención**: La Organización evita en la medida de lo posible, los incidentes de seguridad que puedan perjudicar a la información o a los servicios, mediante la implementación de las medidas especificadas por el ENS, las indicadas desde el entorno del Sistema de Gestión de Seguridad, y adicionalmente, cualquiera que sea considerada necesaria por el Área interna encargada de la gestión de la seguridad que puedan derivarse del análisis y evaluación de riesgos, vulnerabilidades y amenazas, identificando los responsables involucrados.
- **Detección**: Se realizan seguimientos sobre la actividad diaria, para la detección de incidentes y anomalías según lo indicado en el Artículo 9 del ENS, estableciendo mecanismos que permitan la identificación activa, el análisis y el reporte de estos a los responsables designados.
- **Respuesta**: Se dispone de procesos que posibiliten la respuesta frente a los incidentes, contando con vías de comunicación claras a disposición de las partes interesadas, y el intercambio de información en los casos necesarios con las unidades que puedan responder a emergencias.
- **Conservación**: La disponibilidad de los servicios y la información se garantiza a través de planes de continuidad.

5. Requisitos de Seguridad de la Información

Mediante la presente política de seguridad, **ZENER** articula la gestión continuada de la Seguridad de la Información, de acuerdo con los siguientes **requisitos básicos**:

a) **Organización e implantación del proceso de seguridad.** La organización depende de los sistemas TIC para alcanzar los objetivos. Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para su consecución, la organización desarrollo y mantiene un proceso de seguridad basado en los siguientes elementos: **Prevención, Detección, Respuesta y Conservación**.

b) **Análisis y gestión de los riesgos.** Todos los sistemas sujetos a esta Política están sujetos a un análisis de riesgos, según procedimiento interno, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá regularmente, al menos una vez al año, cuando cambie la información manejada, cuando cambien los servicios prestados, cuando ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

c) **Integridad y actualización del sistema.** Todos los sistemas se mantienen íntegros y actualizados según los requisitos establecidos, y gestión a través de procesos de gestión del cambio y análisis de riesgos.

d) **Gestión de personal.** Se establecen los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

Profesionalidad: la seguridad del sistema de información esta atendida y es revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. Se disponen determinados los requisitos de formación y experiencia necesarias del personal para el desempeño de las competencias.

e) **Autorización y control de acceso.** Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

Principio de mínimo privilegio: los sistemas de información han sido diseñados y configurados otorgando los mínimos privilegios necesarios para su correcto desempeño.

f) **Seguridad física y ambiental.** de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

g) **Gestión de activos de información:** inventariados, categorizados y asociados a un responsable.

h) **Protección de la información almacenada y en tránsito.** Toda la información es almacenada de forma adecuada, siguiendo directrices establecidas, en todas sus fases. El sistema protege el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Se almacenan copias de seguridad de manera segura.

i) **Adquisición de productos.** Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

j) **Registro de actividad.** Se registra las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

k) **Gestión de incidentes de seguridad.** Implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

l) **Continuidad del negocio.** Implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información, manteniendo la continuidad de sus procesos de negocio y realizando pruebas periódicas del plan de continuidad.

m) **Mejora continua del proceso de seguridad.** El proceso integral de seguridad implantado es actualizado y mejorado de forma continua. Para ello, se aplican los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

6. Roles y responsabilidades

La organización de la seguridad se articula desde la creación del **Comité de Seguridad TIC**, que queda conformado por los siguientes perfiles: Dirección Responsable del Sistema de Información, Responsable de Seguridad de la Información, Responsable de Sistemas, Responsable de la Información y Responsable del Servicio, que a su vez actúa en la función de secretaría, convocando las reuniones necesarias con registro de estas mediante actas.

Las **funciones del Comité de Seguridad TIC** serán las siguientes:

- En los casos necesarios, reportará al Comité de Dirección
- Coordinar y aprobar las acciones pertinentes en materia de seguridad
- Promover la concienciación y formación en seguridad de la información
- Definir la categoría del Sistema y el análisis de riesgos
- Revisión y aprobación conjunta de la documentación relacionada con la seguridad, así como de los registros asociados
- Participar en la resolución de problemas y discrepancias relacionadas con la gestión de la seguridad.
- Resolver los conflictos de responsabilidades en materia de seguridad de la información que puedan surgir.

Las responsabilidades de la **Dirección Responsable del Sistema de Información** son:

- Aprobación de la documentación final de la documentación del Sistema de Seguridad
- Promover el desarrollo del Esquema
- Dotar de los recursos económicos necesarios para su desarrollo, así como de la presente Política
- Interlocutor en los casos necesarios con el Comité de Dirección

Las responsabilidades del **Responsable de Seguridad de la Información**, quedan definidas como:

- Mantenimiento de los niveles de seguridad adecuados para la información y servicios bajo alcance
- Gestionar la formación y concienciación en materia de seguridad
- Comprobar que las medidas de seguridad son adecuadas a los objetivos y necesidades de la Organización
- Revisar toda la documentación relacionada con la seguridad del sistema
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y medios de auditoría
- Realizar las auditorías que se considerarán necesarias en función del ENS
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta la resolución, aportando informes para el Comité en los casos relevantes
- Operar y mantener el sistema de información durante todo su ciclo de vida.
- Definir el alance del ENS, identificar los activos, su evaluación en cada dimensión y establecer la categoría del sistema.

- Revisar la evaluación de riesgos y plantear las salvaguardas, así como las medidas
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad
- El Responsable de Seguridad de la Información podría 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, será tomada por el Comité de Dirección.

Las responsabilidades del **Responsable de Sistemas** serán las siguientes:

- Promover y colaborar en las auditorías periódicas según ENS en colaboración con el Responsable de Seguridad
- Describir la documentación relacionada con la seguridad
- Participar en la formación y concienciación en materia de seguridad
- Registrar y realizar el seguimiento de las incidencias de seguridad, así como de los cambios que se puedan originar
- Promover las confluencias entre el SGSI y el Esquema Nacional de Seguridad
- Realizar la evaluación de riesgos y amenazas
- Dar soporte al Responsable del Sistema en la definición del alance del ENS, identificación de los activos, así como en la evaluación de estos.
- Colaborar con el RSI y la Dirección en cualquier tarea relacionada con la seguridad que consideren necesaria.

Las responsabilidades del **Responsable de la Información** serán las siguientes:

- Responsable último del uso que se haga de la información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Aprobación de los niveles de seguridad establecidos.

Las responsabilidades del **Responsable del Servicio** serán las siguientes:

- Responsable de establecer los requisitos de los servicios en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.

Como **Usuarios**, la Organización entiende, a cualquier empleado o a terceros externos en aquellos casos que acontezca, que, para el desempeño de su actividad diaria, dentro de las áreas de negocio de la compañía, requieran la utilización de los Sistemas de Información, debiendo colaborar con el Responsable de Seguridad en todas las actividades que les sean indicadas, así como restringir el uso de los Sistemas según las especificaciones aprobadas por el Responsable de Sistemas. Podrán ser designados como responsables de los activos o de los riesgos, dependiendo de su implicación con los mismos.

La designación de los miembros del Comité de Seguridad TIC, se asimila al Comité de Seguridad descrito por el SGSI, siendo los encargados de cualquier actuación relativa a la seguridad históricamente dentro de la Organización.

Respecto a los datos personales, los datos recogidos dentro de la información relevante al alcance del Esquema Nacional de Seguridad, así como los tratados por los servicios indicados pertenecen a la clasificación de tipología baja, contando la Organización según el cumplimiento exigido dentro del SGSI, con un alto desempeño mantenido mediante auditorías de los requisitos asociados a su tratamiento.

El sistema es sometido a un análisis de riesgos, que evalúa las amenazas y los niveles de riesgo registrados al que se encuentra expuesto con frecuencia anual, siempre y cuando no se produzcan incidentes graves, o cambios que pudieran alterar las condiciones iniciales respecto a la información manejada, los servicios prestados, o la aparición de vulnerabilidades.
Una vez establecidas los controles disponibles para la contención de las amenazas, el riesgo final es considerado como "riesgo residual o trivial", estableciéndose categorías de tratamiento según su nivel.

El desarrollo de esta Política se realiza de manera complementaria a las actividades relacionadas en el ámbito del SGSI, encontrándose a disposición de todo el personal de **ZENER**, y constituyendo un elemento de carácter público que podrá ser comunicado tanto a proveedores como clientes.

Se organizarán jornadas de concienciación e información en seguridad para los empleados de Organización, el personal con responsabilidad en el uso, operación, o administración de sistemas TIC, recibirán la formación necesaria en las medidas de seguridad necesarias en cada caso.

En los casos en lo que **ZENER**, utilice a terceros para la provisión de servicios bajo alcance, transmitirá sus requisitos a través de las comunicaciones establecidas en los "Criterios de Evaluación", clasificando a los proveedores según las características establecidas en el mismo.

Se proporcionará una vía de comunicación para que puedan transmitir de manera rápida y directa cualquier incidencia de seguridad relacionada con el servicio o la información objeto de su prestación de servicios. Cuando alguna de las terceras partes, no cumpla con los requisitos mínimos recogidos en los "Criterios de Evaluación" anteriormente citados, se solicitará su reprobación al responsable del área de negocio afectada.

ZENER desarrolla su actividad con plena observancia de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.

La resolución de conflictos de intereses y de interpretación de la Política de Seguridad será competencia del Comité de Seguridad.

Para la coordinación y resolución de conflictos, la organización emplea las juntas tanto ordinarias como extraordinarias del Comité de Seguridad. En la Dirección Responsable del Sistema recae la responsabilidad última en la resolución.

7. Marco normativo

El **Marco Normativo** aplicable a la presente Política, está sometido a revisión periódica, por procedimiento interno, con una periodicidad mínima anual, y es el siguiente:

- ✓ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ✓ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- ✓ 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.
- ✓ Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- ✓ Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- ✓ Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- ✓ Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- ✓ Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- ✓ 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- ✓ Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ✓ UNE-ISO/IEC 27002:2022 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- ✓ UNE-ISO/IEC 27001:2022 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ✓ UNE-EN-ISO 9001:2015 Sistemas de gestión de la calidad.
- ✓ Procedimiento operativo de Gestión de la Seguridad de la Información (ENS).
- ✓ Guías CCN-STIC.
- ✓ Listado documentos del sistema en vigor, procedimientos, normativas e instrucciones técnicas de seguridad.

Marco normativo complementario para Países Bajos:

- ✓ Ley de Protección de Datos Personales (Wet bescherming persoonsgegevens - Wbp): Aunque fue reemplazada por el GDPR, la Wbp (Ley de Protección de Datos Personales) sigue siendo relevante en el contexto histórico y de transición hacia el cumplimiento del GDPR 2.
- ✓ Ley de Ciberseguridad (Wet beveiliging netwerk- en informatiesystemen): Esta ley nacional implementa la Directiva NIS (Directiva (UE) 2016/1148) y establece requisitos específicos para la seguridad de las redes y sistemas de información en los Países Bajos.
- ✓ Ley de Telecomunicaciones (Telecommunicatiewet): Regula aspectos de la seguridad de la información en el sector de las telecomunicaciones, incluyendo la protección de datos y la privacidad de las comunicaciones electrónicas.
- ✓ Ley de Protección de Datos en el Sector Público (Wet politiegegevens - Wpg): Regula el tratamiento de datos personales por parte de las autoridades policiales.

- ✓ Ley de Protección de Datos en el Sector de la Salud (Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - Wabvpz): Establece normas adicionales para el tratamiento de datos personales en el sector de la salud.

Marco normativo complementario para Chile:

- ✓ Ley N° 19.628 sobre Protección de la Vida Privada: Esta ley regula el tratamiento de datos personales y establece los derechos de los titulares de los datos, así como las obligaciones de los responsables del tratamiento. A partir del 01 de diciembre de 2026 regirán las modificaciones introducidas por la Ley 21.719, que moderniza la regulación sobre datos personales, crea derechos como la portabilidad y supresión, y establece la Agencia de Protección de Datos como entidad fiscalizadora.
- ✓ Ley N° 20.285 sobre Acceso a la Información Pública: Aunque se centra en la transparencia y el acceso a la información pública, también incluye disposiciones sobre la protección de datos personales en el sector público. Asimismo, es aplicable a los actores del sector de las telecomunicaciones, en atención de su relación con los titulares de concesiones públicas de telecomunicaciones.
- ✓ Ley Nº 21.663 Marco de Ciberseguridad, que crea la Agencia Nacional de Ciberseguridad (ANCI) y establece obligaciones para organismos públicos y privados respecto a la prevención, reporte y gestión de incidentes de ciberseguridad.
- ✓ Norma Técnica de Seguridad de la Información (NCh-ISO/IEC 27001): Esta norma chilena adopta la ISO 27001 y proporciona un marco para la gestión de la seguridad de la información en las organizaciones.
- ✓ Ley N° 21.180 sobre Transformación Digital del Estado: Esta ley promueve la digitalización de los servicios públicos y establece requisitos para la seguridad de la información en el sector público. El Decreto 7 de 2023 del Ministerio Secretaría General de la Presidencia complementa a esta ley en lo relativo a la norma técnica de seguridad de la información y ciberseguridad, incluyendo la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) y controles técnicos conforme a estándares como ISO/IEC 27001.

8. Cumplimiento y sanciones

El incumplimiento de esta política puede resultar en medidas disciplinarias, tal y como se recoge en el *Dosier de Seguridad de la Información*, incluyendo la terminación del contrato laboral o comercial. La empresa se reserva el derecho de tomar acciones legales en caso de incumplimientos graves.

9. Revisión y aprobación

Esta política será revisada anualmente y aprobada por la alta dirección. Las revisiones serán documentadas y comunicadas a todas las partes interesadas.

Nombre del documento: Política de Seguridad de la Información
Versión: 5.0
Fecha: 18/06/2025
Revisión: anual
Aprobado por: Comité de Seguridad de la Información

D. Enrique de Frutos Encinas
Director General de Zener