



**POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN**

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 1 de 6

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



**POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN**

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 2 de 6

ÍNDICE

1. OBJETIVO	3
2. ALCANCE.....	3
3. ROLES Y RESPONSABILIDADES	3
4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.....	4
5. OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN	4
6. DIRECTRICES ESPECÍFICAS DE SEGURIDAD.....	5
7. SANCIONES	6
8. CONTROL DE CAMBIOS.....	6
9. APROBACIÓN	6



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 3 de 6

1. OBJETIVO

El objetivo de esta política es establecer los principios generales para proteger la confidencialidad, integridad y disponibilidad de la información, conforme con los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y en alineación con la norma ISO/IEC 27001:2022.

Establecer los requisitos y acuerdos relacionados con la seguridad de la información, asegurar la difusión de las políticas internas sobre el uso de la información, comunicados de las aplicaciones permitidas y el compromiso de capacitar a los colaboradores en materia de seguridad de la información

Así como también: Asegurar el Cumplimiento Normativo, Reglamentario y Contractual.

2. ALCANCE

Esta política aplica a:

- Toda la información y los activos de información de TNS Chile incluyendo información digital, impresa, verbal, y los sistemas, redes, aplicaciones y dispositivos que la procesan, almacenan o transmiten.
- Todos los empleados, contratistas, proveedores y terceros que tienen acceso o procesan información en nombre de TNS Chile.
- Todos los procesos de Servicio de Gestión Integral en tecnologías de la información”, Data center y Mesa de ayuda

3. ROLES Y RESPONSABILIDADES

Alta Dirección: Es la responsable de la seguridad de la información en TNS Chile, otorgando los recursos necesarios para su correcto funcionamiento y son los encargados de supervisar la eficacia del SGSI.

Gerencia de TI y Seguridad: Es responsable de la implementación, operación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI), así como de la gestión de incidentes y la aplicación de los controles técnicos.



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 4 de 6

Jefes de Área: Son responsables de garantizar que el personal bajo su cargo comprenda y cumpla con esta política, además son los responsables de generar los procedimientos, controles y protocolos de seguridad de la información y velar por el cumplimiento de estos.

Todos los Empleados: Son responsables de proteger la información a la que tienen acceso, cumplir con las políticas, procedimientos, controles y protocolos de seguridad de la información, y reportar cualquier sospecha de incidente de seguridad.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

TNS Chile se compromete a:

Proteger la Confidencialidad: Asegurar que la información sea accesible y revelada solo a aquellos individuos, entidades o procesos que están autorizados. Esto es crítico para la información de clientes, estrategias comerciales y datos personales.

Mantener la Integridad: Garantizar la exactitud y completitud de la información y los métodos de su procesamiento. Esto asegura la fiabilidad de los datos comerciales y de servicio al cliente.

Asegurar la Disponibilidad: Garantizar que la información y los servicios de información sean accesibles y utilizables cuando se requieran por parte de los usuarios autorizados. Esto es esencial para la continuidad de las operaciones comerciales y la atención al cliente.

5. OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información busca alcanzar los siguientes objetivos:

Cumplimiento Legal y Regulatorio: Asegurar el cumplimiento de todas las leyes, regulaciones y requisitos contractuales relevantes en materia de seguridad de la información y protección de datos. Ley N° 19.628 Protección de datos personales, Ley Marco de Ciberseguridad N° 21.663 y Ley N° 21.459 Normas sobre los delitos informativos entre otras.

Gestión de Riesgos: Identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información de manera sistemática, implementando controles adecuados para mitigar su impacto.



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 5 de 6

Continuidad del Negocio: Minimizar el impacto de incidentes de seguridad en las operaciones de negocio, particularmente en la gestión comercial y el servicio al cliente, a través de planes de continuidad del negocio y recuperación ante desastres.

Conciencia y Capacitación: Fomentar una cultura de seguridad de la información a través de la capacitación y sensibilización de todo el personal.

Reporte de Incidentes: Establecer un proceso claro para el reporte, gestión y resolución de incidentes de seguridad de la información.

Seguridad en la Adquisición: Integrar la seguridad desde el diseño en la adquisición y mantenimiento de sistemas y aplicaciones.

Protección de Datos del Cliente: Asegurar la máxima protección de la información personal y comercial de nuestros clientes.

6. DIRECTRICES ESPECÍFICAS DE SEGURIDAD

Esta política general es complementada por procedimientos y estándares específicos que detallarán aspectos como:

Control de Accesos lógicos: Gestión de usuarios, contraseñas, privilegios y acceso a la red y sistemas.

Seguridad de la información de RRHH: proteger los datos más sensibles de la organización y mitigar los riesgos asociados con el factor humano

Seguridad Física y del Entorno: Protección de las instalaciones, equipos y medios de almacenamiento de información.

Seguridad en las Relaciones con Proveedores: Requisitos de seguridad para la selección y gestión de proveedores que manejan información de TNS Chile.

Gestión de Incidentes de Seguridad de la Información: Procedimientos para la detección, reporte, evaluación y respuesta a incidentes.

Gestión de la Continuidad del Negocio: Planes y pruebas para asegurar la continuidad de las operaciones críticas.

Monitoreo, auditoría y Mejora Continua: Evaluar y fortalecer continuamente la postura de seguridad De TNS, identificando proactivamente las brechas en los controles existentes para implementar mejoras que mitiguen riesgos y aseguren la protección de los activos de información.



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: SGSI-PO-01

Elaborado: 03/07/2025

Página: Página 6 de 6

7. SANCIONES



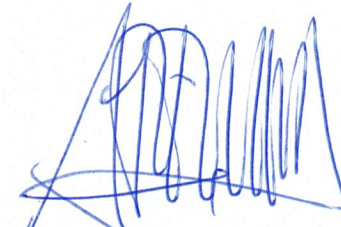
El incumplimiento de esta Política y los procedimientos de seguridad de la información asociados puede resultar en acciones disciplinarias que se encuentran descritas en el artículo n°66 del Reglamento de Orden Higiene y Seguridad.

8. CONTROL DE CAMBIOS

Esta Política será revisada anualmente, o antes si ocurren cambios significativos en el negocio, los sistemas de información, los riesgos de seguridad o los requisitos legales/regulatorios, para asegurar su continua idoneidad, suficiencia y eficacia.

VERSIÓN	FECHA	COMENTARIO DE LA MODIFICACION	RESPONSABLE
02	03-07-2025	Separación de la política de seguridad de información como documento independiente de TNS	

9. APROBACIÓN

ELABORADO POR	APROBADO POR	APROBADO POR
 Sebastian Pardo A.	 Rodrigo Barrios S.	 Sergio Araya A.
Auditor Interno	Director de Comercial e Inteligencia de Negocio	Director de Operaciones e Ingeniería