



Extracto Público de Políticas de Seguridad de la Información

SIGNOVA SPA POL-SGSI-4.1v1.1

24-09-2026

1. Introducción

En este documento se establece un extracto público de las políticas de seguridad de la información y del Sistema de Gestión de Seguridad de la Información (SGSI) de SIGNOVA SPA, con el propósito de comunicar a las partes interesadas externas los principios, compromisos y directrices fundamentales que guían nuestras acciones en materia de seguridad de la información.

Su implementación no solo busca cumplir con estándares y regulaciones, sino también fortalecer la capacidad de la organización para identificar, mitigar y responder eficazmente a los riesgos de seguridad que puedan afectar la confidencialidad, integridad y disponibilidad de la información sensible y estratégica, generando confianza en clientes, proveedores y demás partes interesadas.

2. Objetivo

El objetivo de este documento es comunicar de manera clara y transparente a las partes interesadas externas —clientes, proveedores, contactados, autoridades reguladoras, auditores y demás terceros relevantes— los lineamientos generales de seguridad aplicados por SIGNOVA SPA para proteger sus activos y garantizar la confidencialidad, integridad y disponibilidad de su información, alineados a la misión, visión y valores de la organización, así como a los requisitos de la norma ISO/IEC 27001:2022.

3. Alcance

El presente extracto es aplicable a todas las partes interesadas externas que mantengan una relación comercial, contractual o funcional con SIGNOVA SPA y que, en el marco de dicha relación, accedan a información o activos de la organización, o entreguen información para su tratamiento.

El alcance del Sistema de Gestión de Seguridad de la Información de SIGNOVA SPA, contempla por medio de controles técnicos asegurar los datos y documentación de las tareas y entregables que el cliente espera como resultado, tanto para los procesos de firmas presencial y electrónica, validación y despacho de set de documentos originales recepcionados en nuestras instalaciones, proceso de Pagarés que implica, impresión, validación, gestión de firma notario, legalización y envío carta de notificación al cliente final, cumpliendo con confidencialidad, integridad y disponibilidad de la información, tanto para el cliente interno como el cliente final. De acuerdo con declaración de aplicabilidad del 06 de diciembre 2025".

Los controles aplicables se encuentran documentados en la Declaración de Aplicabilidad (SoA) vigente del SGSI.

8. Contenido

Declaración de compromiso de la Alta Dirección

La Gerencia General de SIGNOVA SPA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus servicios con sus clientes y proveedores, en cumplimiento de las leyes aplicables y en concordancia con la misión y visión de la entidad.

La Seguridad de la Información en SIGNOVA SPA es parte fundamental del negocio para así entregar confianza a sus clientes y usuarios sobre las tecnologías de la información que opera. La información, basada en nuestra clasificación, se gestiona con los más altos estándares según las mejores prácticas disponibles en el mercado, constituyéndose en una base para el crecimiento y sostenibilidad organizacional.

Principios rectores

La gestión de la seguridad de la información en SIGNOVA SPA se fundamenta en los siguientes principios:

- Confidencialidad: la información es accesible únicamente a quienes están autorizados.
- Integridad: la información se mantiene exacta, completa y libre de alteraciones no autorizadas.
- Disponibilidad: la información y los servicios que la soportan están disponibles cuando se requieren.
- Cumplimiento: todas las actividades se desarrollan en cumplimiento de la legislación y regulaciones aplicables.
- Enfoque basado en riesgos: las decisiones de seguridad se toman con base en análisis formales de riesgo.
- Mejora continua: el SGSI se evalúa y perfecciona de manera permanente.

Compromisos de SIGNOVA SPA

La Gerencia General de SIGNOVA SPA asume y comunica los siguientes compromisos frente a sus partes interesadas:

Compromiso	Descripción
Confidencialidad, integridad y disponibilidad (CID)	Proteger la información de nuestros clientes contactados y partes interesadas frente a accesos no autorizados, alteraciones indebidas e indisponibilidad, aplicando controles técnicos y organizativos proporcionales al nivel de riesgo y clasificación de la información.
Protección de datos personales	Tratar los datos personales conforme a la legislación vigente, aplicando medidas de cifrado, control de acceso, enmascaramiento, auditoría y trazabilidad sobre toda operación que involucre datos sensibles.
Gestión de riesgos	Identificar, evaluar y tratar los riesgos de seguridad de la información de manera formal, periódica y documentada, incluyendo la gestión de riesgos asociados a proveedores y servicios en la nube.
Continuidad operativa	Mantener planes de continuidad del negocio y recuperación ante desastres que aseguren la prestación de los servicios críticos ante eventos inesperados.
Gestión de incidentes	Disponer de un proceso formal para la recepción, análisis, tratamiento y comunicación de incidentes de seguridad, incluyendo la notificación oportuna a las partes afectadas y autoridades competentes cuando corresponda.
Cumplimiento legal y contractual	Cumplir con la legislación chilena aplicable y con los compromisos contractuales asumidos con clientes y proveedores en materia de seguridad de la información.
Concientización y competencia	Capacitar y concientizar de forma continua a los colaboradores internos y externos sobre sus responsabilidades en seguridad de la información.
Mejora continua	Evaluar periódicamente el desempeño del SGSI mediante auditorías, indicadores y revisiones por la dirección, promoviendo acciones correctivas y de mejora.

Obligaciones y expectativas hacia partes interesadas externas

SIGNOVA SPA espera que las partes interesadas externas que mantengan una relación comercial, contractual o funcional con la organización cumplan con las siguientes obligaciones en materia de seguridad de la información:

Obligación	Descripción
Confidencialidad	Proteger toda información entregada o accedida en el marco de la relación con SIGNOVA SPA, utilizándola exclusivamente para los fines acordados y no divulgándola a terceros no autorizados.
Uso adecuado de accesos	Utilizar las credenciales y accesos otorgados de manera personal e intransferible, sin compartir contraseñas ni delegar accesos, y aplicando medidas de autenticación reforzada cuando así se requiera.
Reporte de incidentes	Comunicar de forma oportuna cualquier incidente, sospecha de incidente, vulnerabilidad o anomalía de seguridad detectada, a través de los canales establecidos por SIGNOVA SPA.
Cumplimiento de políticas aplicables	Conocer y cumplir las políticas, procedimientos y cláusulas contractuales de seguridad de la información que les sean comunicadas por SIGNOVA SPA.
Protección de datos personales	Tratar los datos personales a los que accedan conforme a la legislación vigente y a los acuerdos contractuales suscritos, garantizando su resguardo y no divulgación.
Propagación a la cadena de suministro	Cuando corresponda, los proveedores deberán trasladar los requisitos de seguridad de SIGNOVA SPA a sus subcontratistas o terceros involucrados en la prestación del servicio.

El incumplimiento de estas obligaciones podrá derivar en la revisión, suspensión o término de la relación, así como en las acciones legales que correspondan conforme a los contratos suscritos y a la legislación vigente.

Canal de reporte y contacto

SIGNOVA SPA pone a disposición de sus partes interesadas externas los siguientes medios para reportar incidentes de seguridad, vulnerabilidades, consultas o solicitudes relacionadas con el presente documento:

- Correo electrónico institucional de seguridad de la información:
ciberseguridad@Signova.cl
- Contacto con el Oficial de Seguridad de la Información a través de los canales formales establecidos contractualmente.

Toda comunicación recibida será tratada conforme a los procedimientos internos de gestión de incidentes y atención a partes interesadas del SGSI.

Revisión y vigencia

Este extracto es revisado y actualizado al menos una vez al año, o cuando ocurran cambios significativos en el SGSI, en la legislación aplicable o en el contexto organizacional. La versión vigente será la publicada oficialmente por SIGNOVA SPA y comunicada a las partes interesadas a través de los canales oficiales de la organización (Página web, correo electrónico, wsp de contacto o Link dinámico por correo electrónico)

Este documento entra en vigencia a partir de su fecha de aprobación por la Gerencia General y permanece vigente hasta su próxima revisión formal.