



Política de Seguridad de la información

Sistema Gestión de Seguridad, Ciberseguridad y Privacidad de la Información

PRENDA CHILE comunica a sus colaboradores, clientes, proveedores y aliados estratégicos la adopción y formalización de su Política de Seguridad de la Información, diseñada para resguardar la confidencialidad, integridad y disponibilidad de los datos que gestionamos.

Este marco normativo establece principios y responsabilidades que fortalecen nuestra cultura organizacional y garantizan el cumplimiento de estándares nacionales e internacionales. Con esta iniciativa, reafirmamos que la seguridad de la información es un pilar estratégico para la confianza, la transparencia y la continuidad de nuestras operaciones, invitando a todos los actores internos y externos a conocer, difundir y aplicar esta política en el desarrollo de sus actividades.

Atentamente,

Política de Seguridad de la Información de Prenda Chile

Estimados clientes, proveedores y partes interesadas:

En Prenda Chile protegemos la información que nos confían. Por eso contamos con una Política de Seguridad de la Información, aprobada por nuestro Comité del Sistema de Gestión de Seguridad de la Información (SGSI) y basada en la norma internacional ISO/IEC 27001:2022. A continuación resumimos sus principales compromisos.

- 1. Objetivo y alcance** La política busca proteger la confidencialidad, la integridad y la disponibilidad de la información en todo su ciclo de vida, desde que se crea hasta que se destruye. Se aplica a todos nuestros sistemas y áreas, y a todas las personas, internas o externas, que usan información de Prenda Chile.

2. Protección de datos personales

- Tratamos los datos personales de forma lícita, leal y transparente, conforme a la Ley N° 19.628, modificada por la Ley N° 21.719.

- Solo recolectamos los datos necesarios para la finalidad informada, los guardamos solo durante el plazo requerido y después los eliminamos o anonimizamos de forma segura.
- Los titulares pueden ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y bloqueo a través de un canal habilitado para ello.
- Contamos con un encargado de protección de datos personales. Si ocurre un incidente que afecte datos personales, lo notificamos a la autoridad y a los afectados cuando la ley lo exige.

3. Control de acceso

- Cada persona accede solo a la información que necesita para su función.
- Las cuentas son personales. Usamos autenticación multifactor en los sistemas críticos y revisamos los accesos periódicamente.
- Los accesos de terceros son temporales y se limitan al servicio contratado.

4. Clasificación y manejo de la información Clasificamos la información como Reservada, Confidencial, Interna o Pública, y la protegemos según su nivel. Cuando un activo ya no se necesita, lo borramos o destruimos de forma segura.

5. Seguridad tecnológica y física Mantenemos protección contra software malicioso, gestión de vulnerabilidades con pruebas de seguridad al menos una vez al año, redes segmentadas, comunicaciones cifradas y controles físicos en nuestras instalaciones.

6. Relación con proveedores

- Todo proveedor firma un contrato que incluye obligaciones de seguridad y confidencialidad y el compromiso de cumplir nuestras políticas.
- Evaluamos a nuestros proveedores cada seis meses.
- Pedimos que estos requisitos se trasparen a sus propios subcontratistas.
- Si un servicio en la nube guarda información sensible, esta debe permanecer cifrada, y el servicio se contrata solo después de evaluar sus riesgos.

7. Gestión de incidentes Colaboradores, clientes y proveedores deben informarnos de cualquier incidente de seguridad, confirmado o posible. Registramos, analizamos y resolvemos cada caso según un procedimiento formal. También mantenemos contacto con organismos como la ANCI, el CSIRT de Gobierno y la Unidad de Cibercrimen de la PDI.

8. Continuidad del negocio Contamos con planes de continuidad y de recuperación ante desastres, que probamos y actualizamos periódicamente, para mantener disponibles nuestros servicios clave.

9. Cumplimiento y mejora continua Identificamos las leyes, normas y contratos que nos aplican, y revisamos el cumplimiento del SGSI cada seis meses mediante auditorías internas. Además, capacitamos a nuestros colaboradores cada año.

Para consultas sobre esta política o para informar un incidente de seguridad, escribanos al correo electrónico ciberseguridad@prendachile.cl

Santiago de Chile, 06 de octubre de 2026.