



Dos leyes, una solución: Prey

Te ayudamos a cumplir fácilmente
con las leyes Marco de Ciberseguridad
(21.663) y Protección de Datos (21.719)



El nuevo escenario en Chile

La ciberseguridad y la protección de datos ya no son opcionales para empresas en Chile: hoy son obligaciones legales que pueden significar altos costos por incumplimiento. Urge crear alianzas estratégicas para proteger dispositivos, datos y respaldos con evidencia y reportería.

Las nuevas leyes de Ciberseguridad y PDP exigirán serios estándares a todas las empresas que califican como PSE u OIV:

Un prestador de servicios esenciales (PSE) es una entidad cuya operación es crítica para el país (salud, abastecimiento, servicios básicos, etc.) y por eso la Ley 21.663 le exige medidas concretas de ciberseguridad.

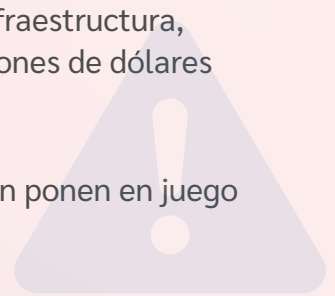
Un operador de importancia vital (OIV) es un caso aún más exigente: su dependencia tecnológica y el impacto de un incidente pueden afectar gravemente la continuidad del servicio o la seguridad pública.

¿Qué significa este nuevo escenario normativo?

- **Ley Marco de Ciberseguridad (21.663):** Esta ley obliga a las entidades críticas a implementar un Sistema de Gestión de Seguridad de la Información (SGSI), reportar incidentes y mantener auditorías continuas. El incumplimiento promete multas de hasta 40.000 UTM y sanciones administrativas.
- **Ley de Protección de Datos Personales (21.719):** Esta ley reconoce los datos personales como un derecho fundamental. Las empresas deben tener respaldo de sus políticas de resguardo de datos personales, de lo contrario arriesgan multas económicas severas.

En conjunto, estas leyes redefinen cómo las empresas deben proteger infraestructura, información y reputación. Están en juego sanciones superiores a 2,6 millones de dólares por incumplimiento.

Además del dinero, las empresas que no cumplan con estas leyes también ponen en juego la confianza de sus clientes, pacientes, estudiantes o ciudadanos.



Las leyes en mayor detalle

 Ley 21.663 – Ciberseguridad	 Ley 21.719 – Protección de Datos Personales
 Gestión continua de la seguridad: Mantener un SGSI robusto con análisis de riesgos y planes de mitigación. Debe incluir la eliminación de cuentas inactivas.	 Protección de datos como derecho fundamental: Resguardar datos personales y sensibles de clientes, pacientes, estudiantes o colaboradores.
 Reporte de incidentes: Informar ciberataques y brechas a la Agencia Nacional de Ciberseguridad (ANCI).	 Notificación de brechas: Reportar incidentes de datos a la Agencia de Protección de Datos y a los titulares afectados.
 Registro de auditoría: Mantener registros detallados de las acciones para presentar a la ANCI.	 Derechos ARCO+: Garantizar acceso, rectificación, cancelación, oposición y portabilidad de los datos.
 Sanciones importantes: Multas de hasta 40.000 UTM en caso de incumplimiento.	 Sanciones económicas y civiles: Multas proporcionales a la gravedad y responsabilidad civil en caso de daños.
 Medidas de seguridad obligatorias: Implementar controles técnicos y organizativos para garantizar continuidad operativa y resiliencia cibernética. Todas las cuentas deben usar autenticación multifactor (MFA), y todo acceso remoto tiene que incluir el uso de VPN institucional.	 Medidas de seguridad obligatorias: Implementar controles técnicos y organizativos que eviten filtraciones o accesos indebidos.
 Nuevas figuras: Creación de la ANCI y obligación de designar Delegado/Encargado de Ciberseguridad.	 Nuevas figuras: Creación de la Agencia de Protección de Datos Personales como autoridad independiente y fiscalizadora.

Los plazos que debes conocer y cumplir



Plazos de cumplimiento y prevención

- **Implementación Inicial:** Las empresas tienen **60 días corridos** desde su calificación como OIV para cumplir con las medidas de contención obligatorias.
- **Mantenimiento preventivo:** Es obligatorio eliminar cuentas administrativas genéricas o inactivas al menos cada **6 meses**.



Respuesta ante incidentes (Ventana de 3 Horas)

Tras detectar un incidente, las siguientes acciones deben ejecutarse en un máximo de 3 horas:

- **Contención crítica:** Cambiar contraseñas administrativas y bloquear accesos remotos o expuestos.
- **Reporte a la ANCI:** Informar el hallazgo detallando los horarios exactos de detección y las medidas de mitigación aplicadas.



Medidas de aislamiento inmediato

Acciones inmediatas para detener la propagación del ataque:

- **Restricción y aislamiento:** Limitar accesos a sistemas comprometidos y separar la infraestructura afectada del resto de la red.
- **Suspensión de funciones:** Deshabilitar temporalmente integraciones y accesos remotos que faciliten la expansión del incidente.

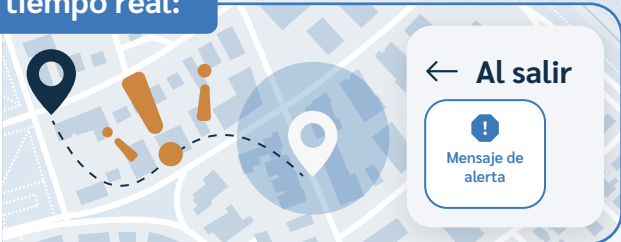
Todo esto debe ser comprobable con la documentación correspondiente.

Cumple con estas nuevas leyes con la ayuda de Prey

Prey combina gestión de dispositivos, protección de información y evidencia lista para ser auditada, facilitando el cumplimiento de ambos marcos legales. A continuación detallamos algunas funcionalidades que te cubren ante estas nuevas regulaciones:

1. Para obtener visibilidad y control de activos en tiempo real:

- Geolocalización y geocercas:** Siempre sabrás dónde están tus equipos. Prey te permite configurar zonas de seguridad que activan alertas y acciones automáticas si un dispositivo se sale de ellas; obtienes detección proactiva.



2. Para dar respuesta inmediata y prevenir brechas:

- Bloqueo y borrado remoto:** Actúa al instante para proteger tu información. Prey bloquea dispositivos y los borra remotamente para evitar acceso no autorizado.
- Cifrado de disco (BitLocker):** Para dispositivos Windows, puedes gestionar el cifrado de disco remotamente, inhabilitando los datos incluso ante equipos robados.
- Breach Monitoring:** El servicio revisa continuamente y detecta si tus credenciales se han filtrado en la Dark Web, lo que te permite actuar sobre datos filtrados antes de que sean utilizados y se conviertan en una brecha de seguridad.



3. Para reunir evidencia y prepararte en caso de auditorías:

- **Prey genera informes de evidencia vitales para los reportes que exige la ley.** En caso de incidente, puedes obtener:
 - Ubicación, información de red e IP.
 - Fotografías y capturas de pantalla del equipo.
- **El registro de auditoría** de Prey te permite llevar un historial de todas las acciones y cambios, demostrando que cumples ante la ANCI.



Cómo Prey te ayuda a cumplir las nuevas regulaciones

Exigencia Legal	Cómo ayuda Prey	Impacto financiero
Ley 21.663 (Ciberseguridad): Implementar SGSI y reportar incidentes a la ANCI.	Registro de auditoría con historial de acciones, reportes automáticos con información como ubicación, red e IP.	✓ Evidencia inmediata → evita sanciones por incumplimiento (hasta 40.000 UTM ≈ USD 2,6M).
Ley 21.663: Proteger continuidad y reaccionar rápido ante incidentes.	Bloqueo y borrado remoto, restablecer de fábrica, y cifrado de discos.	✓ Contención inmediata → evita fuga de datos y costos de recuperación.
Ley 21.719 (Protección de Datos): Garantizar confidencialidad de datos personales.	Cifrado remoto y control de dispositivos extraviados o robados.	✓ Minimiza riesgos legales y de reputación → protege la confianza de clientes, pacientes o alumnos.
Ley 21.719: Reportar y demostrar diligencia ante filtraciones.	Breach Monitoring detecta credenciales expuestas en Dark Web.	✓ Aviso temprano → reduce costos de incidentes, evita multas y pérdida de clientes.
Ambas leyes: Mantener trazabilidad y control de activos.	Inventario centralizado, geocercas, alertas y monitoreo en tiempo real.	✓ Control financiero → menos pérdidas de equipos (200 dispositivos ≈ USD 300K) y datos críticos.

De la norma a la práctica

La **Ley 21.719** establece *qué datos* resguardar.

La **Ley 21.663** establece *qué* debes proteger.

Prey te entrega el cómo: control total de dispositivos, evidencias claras y respuesta rápida ante incidentes.

Prey en distintas versiones

Protección escalable, sin costos ocultos, y listo para crecer con tu equipo. Adapta la seguridad a las necesidades y tamaño de tu organización:

 Tracking	 Protection	 Full Suite	 Breach Monitoring (add-on)
Visibilidad de tu flota con geolocalización y geocercas. Ideal para gestión básica de inventario y control.	Control y respuesta avanzada con bloqueo, borrado remoto y cifrado. Perfecto para cumplir con las leyes 21.663 y 21.719.	Todas las funciones anteriores, más automatización y reportes de cumplimiento. Diseñado para organizaciones bajo altos estándares regulatorios.	Detección de credenciales filtradas en la Dark Web. Tu reporte se actualiza semanalmente.

La confianza de miles de organizaciones a nivel global

Más de 8 millones de dispositivos protegidos y diversas organizaciones a nivel mundial confían en Prey para proteger dispositivos y datos. Conoce nuestra experiencia de compliance mundial.



Somos una empresa con certificación **SOC 2**, una validación que demuestra nuestro compromiso con la seguridad y ayuda a mitigar el riesgo de brechas de seguridad para nuestros clientes.

Prey es valorada como una de las soluciones mejor calificadas en **MDM y Data Protection**, destacando por su facilidad de uso, soporte al cliente y ROI.

Conoce Prey en acción

El mejor momento para fortalecer tu SGSI y tu programa de protección de datos **es ahora.**

Con Prey, el cumplimiento normativo deja de ser un dolor y se convierte en una ventaja competitiva:

- ✓ Control y trazabilidad de tus dispositivos
- ✓ Respuesta inmediata ante incidentes de brechas
- ✓ Evidencias listas para auditorías



[Agenda tu demo guiada y
prepárate para cumplir sin
complicaciones.](#)

Sobre Prey

Nacimos en 2009 con una misión clara: devolverle a las personas el control sobre su tecnología. Hoy, Prey ha evolucionado en una **plataforma integral de gestión y seguridad para flotas globales**.

Más allá del rastreo, empoderamos a las empresas con herramientas avanzadas para el manejo de software, cumplimiento de políticas y protección de datos.

Somos el aliado estratégico que ayuda a administrar y proteger entornos de trabajo remoto, facilitando el cumplimiento normativo. Un equipo comprometido con la continuidad de tu operación.

Prey para: **Personas | Organizaciones | Escuelas y Universidades**

Prey Spa. © Santiago, RM Chile