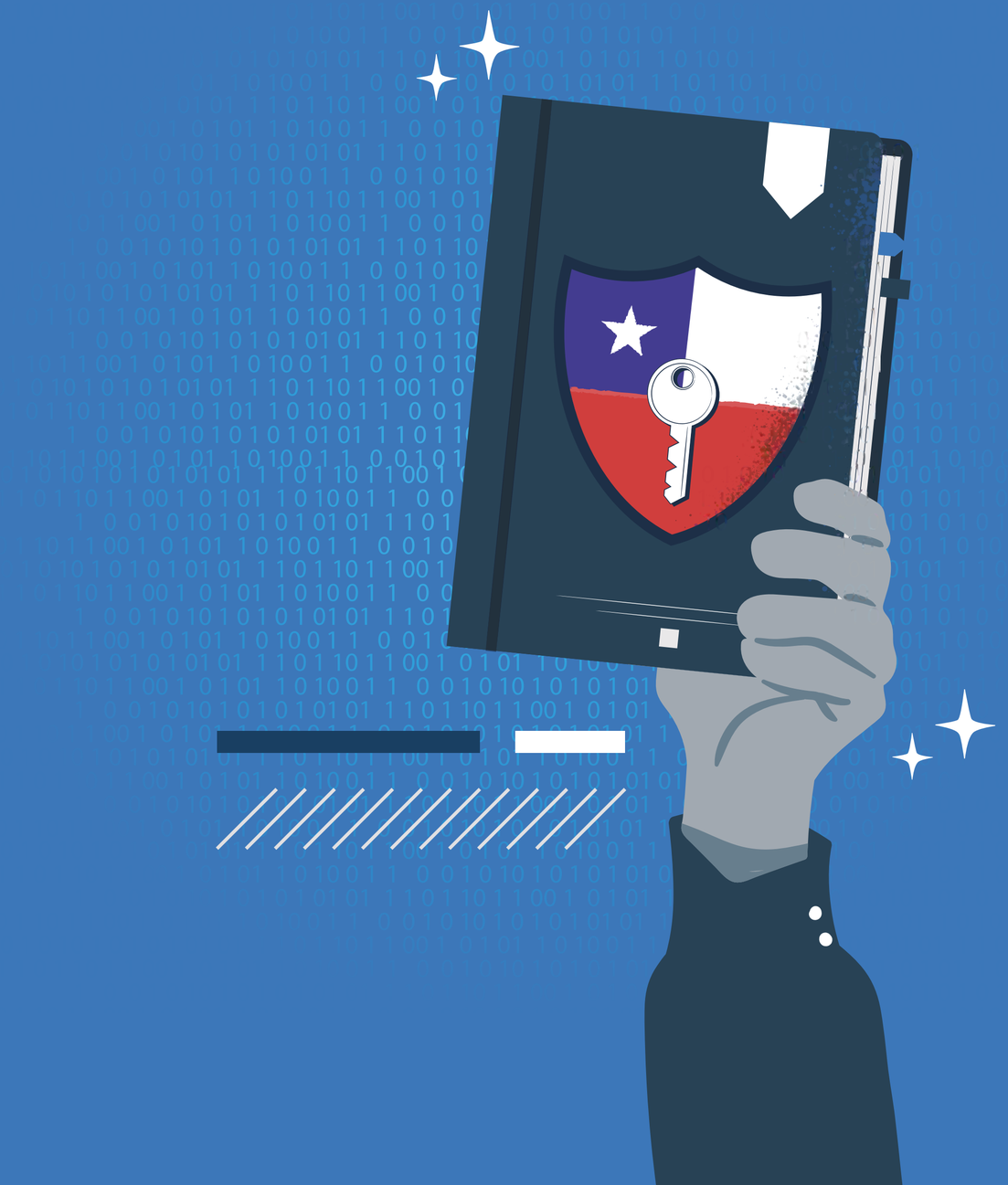
Guía definitiva para cumplir con

la ley 21.663



Prey Inc.

Guía definitiva para cumplir con la ley 21.663

En los últimos años, la ciberseguridad en Chile dejó de ser una preocupación solo para expertos. La creciente cantidad de ataques que afectan servicios públicos, empresas privadas y organismos estatales llevó al país a dar un paso firme con la Ley 21.663 promulgada en abril de 2024. Esta normativa busca establecer reglas claras para proteger la información y la operación de sectores clave.

La Ley está diseñada para resguardar la infraestructura crítica, los servicios esenciales y el orden público frente a amenazas digitales. Esta guía está pensada para organizaciones que podrían estar bajo su alcance: operadores de servicios esenciales, de importancia vital, PYMEs proveedoras de servicios críticos y cualquier entidad que quiera adelantarse a los requisitos y fortalecer su ciberseguridad.

Aumento de hackeos en Chile: alerta por ciberataques y suplantación

Aumento de los ciberataques en Chile en 2023: Lo que dicen las cifras, las formas más frecuentes y las consecuencias

Chile es el segundo país de la región con más ciberataques este año: suma más de un millón

El auge de los ciberataques en Chile: fuga de datos afecta al 60% de las empresas y experta llama a “estar alertas”

Sabías que?

Según Fortinet, Chile sufrió en el 2024 más de 27,600 millones intentos de ciberataques, posicionándose como el segundo país de la región con más ciberataques.

01 Qué regula la ley marco de ciberseguridad

Qué regula la ley marco de ciberseguridad

La Ley 21.663, también conocida como Ley Marco de Ciberseguridad, establece un marco legal para proteger a Chile de ciberataques que podrían paralizar servicios esenciales o comprometer datos críticos. Busca solucionar la falta de coordinación y de estándares claros en la respuesta a incidentes, asegurando que tanto organismos públicos como privados adopten medidas preventivas y reactivas.

La Agencia Nacional de Ciberseguridad (ANCI)

La ley marco crea la ANCI como autoridad encargada de coordinar, supervisar y fortalecer la ciberseguridad en Chile. Actúa como punto central entre el Estado, las empresas y la sociedad para prevenir y gestionar incidentes digitales que puedan afectar servicios críticos o la seguridad pública. Además, define estándares y protocolos técnicos para todos los sectores obligados.

Funciones clave de la ANCI:

- Dictar protocolos y estándares de ciberseguridad.
- Coordinar la respuesta ante incidentes nacionales.
- Fiscalizar y sancionar incumplimientos.
- Mantener un registro de incidentes y vulnerabilidades.
- Promover la cultura de ciberseguridad en el país.

Sectores que entran directo al radar ANCI

La ley define ocho grandes verticales que el Congreso consideró “imprescindibles para la vida del país” (art. 4, inc. 2). Si operas en cualquiera de los siguientes sectores ya estás en el radar:

- Sector público (ministerios, delegaciones regionales y provinciales, municipalidades)
- Salud (hospitales, clínicas, laboratorios)
- Energía (generación, transmisión, distribución)
- Transporte (aéreo, marítimo, terrestre, ferroviario)
- Telecomunicaciones e infraestructura digital
- Banca, servicios financieros y medios de pago
- Suministro de agua potable y saneamiento
- Servicios postales y de mensajería
- Producción e investigación farmacéutica

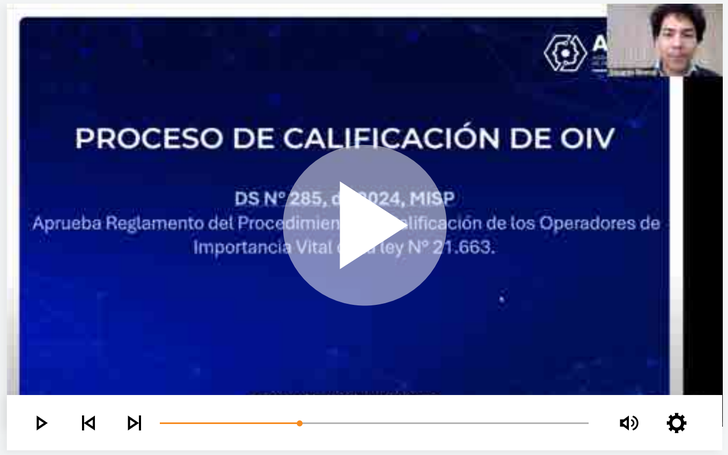
Ojo con la cadena de suministro!
Si prestas un servicio TI gestionado (cloud, datacenter, SaaS) a estos sectores, la ANCI puede designarte OIV “por arrastre” aunque no aparezcas hoy en el Diario Oficial.

Conoce más:
Resolución Nº 24, de 2025 de Agencia Nacional de Ciberseguridad - procedimiento de calificación de Operadores de Importancia Vital.

OSE vs OIV

Los operadores de Servicios Esenciales (**OSE**) y los **Operadores de Importancia Vital (OIV)** son categorías definidas por la Ley 21.663 para identificavar a las organizaciones que deben cumplir obligaciones específicas en ciberseguridad. Ambas categorías agrupan entidades que, por su rol, son fundamentales para el funcionamiento del país y la protección de la ciudadanía.

Característica	OSE (Operadores de Servicios Esenciales)	OIV (Operadores de Importancia Vital)
Definición	Instituciones que prestan servicios críticos para la sociedad.	Entidades cuya afectación, interceptación, interrupción o destrucción de sus servicios afecten significativamente al país (seguridad y orden público).
Ejemplos	Agua, electricidad, transporte, telecomunicaciones.	Centros de datos estratégicos, infraestructura crítica.
Obligaciones principales	Reporte de incidentes, obligaciones generales de ANCI, planes de continuidad.	SGSI, certificaciones, plan de continuidad y respuesta ante incidentes, simulacros periódicos.
Plazos de cumplimiento	Tras publicación de reglamentación técnica los OSE tendrán 12 meses de plazo	Tras publicación de reglamentación técnica los OIV tendrán 24 meses de plazo



Recomendable:
Charla ANCI: “Operadores de Importancia Vital (OIV): Etapas del proceso de calificación”

02

¿Mi organización está obligada a cumplir?

¿Mi organización está obligada a cumplir?

Si tu organización forma parte de un sector crítico —como energía, salud, transporte o telecomunicaciones— es posible que ya seas un Prestador de Servicios Esenciales (OSE) o incluso un Operador de Importancia Vital (OIV). Pero no termina ahí: la ANCI también puede designar como OIV a instituciones privadas que, aunque no sean OSE, cumplen un rol estratégico en el país.

Para definir si un servicio es esencial o de importancia vital, la Agencia sigue un proceso detallado que considera el impacto potencial de su interrupción y su dependencia de redes y sistemas informáticos.

Este procedimiento incluye:

1. Solicitar informes a organismos públicos con competencia en el sector.
2. Elaborar una nómina preliminar de instituciones candidatas.
3. Someter la nómina privada a consulta pública por 30 días.
4. Recibir informe del Ministerio de Hacienda sobre las entidades públicas.
5. Emitir una resolución final que establece oficialmente a los OIV.

Qué pasa si aún no estás designado oficialmente

Aunque tu organización no haya sido designada oficialmente como OSE u OIV, eso no significa que esté fuera de riesgo. La ANCI revisa y actualiza las designaciones cada tres años, y una afectación significativa podría hacer que pases a estar en la lista. Prepararte desde ya es una ventaja para evitar sorpresas y responder mejor ante incidentes.

Auto-chequeo express (responde SÍ/NO)

Pregunta	"sí" significa...
¿Prestamos alguno de los ocho servicios esenciales (salud, energía, transporte, etc.)?	Eres OSE; regístrate ya en portal.anci.gob.cl con tu clave única
¿Una caída total dejaría sin servicio a más de una región o pondría vidas en riesgo?	Criterio de impacto nacional → probable OIV
¿Proveemos TI crítico (cloud, datacenter, SaaS, OT) a clientes OSE/OIV?	Puedes ser nombrado OIV por arrastre; mismas multas
¿Dependemos de un único SCADA, datacenter tier III+ o sistema OT cuya falla frene todo?	Ese punto único de falla es foco directo de fiscalización
¿Gestionamos datos cuyo robo obligaría a notificar según Ley 19.628 o expone riesgo penal Ley 20.393?	La 21.663 se suma a tus deberes de protección y prevención penal.
¿Hemos recibido un oficio o encuesta de la ANCI/CSIRT pidiendo información?	Estás en proceso formal de calificación: prepara SGSI y delegado hoy.

A tomar en cuenta

- **3 o más "SÍ":** Actúa desde ahora como OSE/OIV; las sanciones (hasta 40 000 UTM) aplican en marzo 2025.
- **1-2 "SÍ":** Implementa controles básicos y monitorea nuevas resoluciones ANCI.
- **0 "SÍ":** Mantén buenas prácticas; la lista se actualiza cada tres años.

Consideraciones especiales para PYMEs y proveedores críticos

Las PYMEs y proveedores que forman parte de cadenas de suministro esenciales pueden verse afectados indirectamente. Aunque la ley contempla su tamaño y capacidades, es clave que demuestren buenas prácticas de ciberseguridad para no convertirse en eslabones débiles que comprometan a los grandes operadores. Esto también puede abrirles puertas en contratos y licitaciones.

Consideraciones a tomar:

- Identificar si tus clientes principales son OSE u OIV.
- Designar un encargado/responsable por velar la seguridad
- Adoptar soluciones asequibles como MDM, AV, gestor de contraseñas, firewalls y backups automáticos.
- Capacitar al equipo en ciberhigiene básica.
- Documentar procesos de seguridad, aunque sean simples.
- Tener un plan de continuidad de negocio y respuesta ante incidentes
- Explorar certificaciones o estándares simplificados como ISO 27001 para PYMEs.

03 Obligaciones principales según la ley

Obligaciones principales según la ley

La Ley 21.663 establece un conjunto de obligaciones (artículo °8) para garantizar que las organizaciones críticas puedan **prevenir, detectar y responder a incidentes de ciberseguridad y reportar a CSIRT nacional dichos incidentes con efectos significativos.**

Las medidas aplican principalmente a los OSE y OIV, que deben adoptar prácticas sólidas y comprobables para proteger sus sistemas, datos y la continuidad de sus servicios frente a amenazas crecientes.

A continuación mencionaremos las obligaciones principales:

Registro obligatorio en el portal ANCI

OSE : ✓ | OIV: ✓

Todos los OSE y OIV deben registrarse en la plataforma oficial de la ANCI. Este registro es el punto de partida para que la Agencia los supervise, coordine acciones de ciberseguridad y les notifique sobre estándares o protocolos aplicables. Es un requisito indispensable para demostrar la disposición a cumplir con la normativa.

Desde el 11 de junio del 2025 ya se encuentra abierto las inscripciones en el portal ANCI: **portal ANCI:**

Designación de delegado de ciberseguridad

OSE : R | OIV: ✓

Las organizaciones obligadas deben nombrar un delegado de ciberseguridad que será el enlace directo con la ANCI. Este responsable no solo coordina las acciones internas de seguridad, sino que también se encarga de informar a la alta dirección sobre riesgos y cumplimiento, además de liderar la respuesta ante incidentes.

Implementación de un SGSI activo y documentado

OSE : ✗ | OIV: ✓

Para los OIV, la ley exige un Sistema de Gestión de Seguridad de la Información (SGSI) que no sea solo un conjunto de documentos, sino una práctica continua. Debe incluir políticas, procesos y controles activos para gestionar riesgos y garantizar la confidencialidad, integridad y continuidad de los activos informáticos.

Conoce mas sobre el SGSI aplicado a la ley marco:
Guía práctica sobre SGSI e ISO 27001

Reporte de incidentes (plazo: 3 horas)

OSE : ✓ **OIV:** ✓

Cuando ocurre un incidente de ciberseguridad significativo, los OSE y OIV deben enviar un notificación al **CSIRT Nacional** dentro de los siguientes períodos de tiempo:

- Alerta temprana sobre la ocurrencia dentro de las primeras 3 horas detectado el evento.
- Enviar una actualización de la información más detallada en donde incluya evaluación inicial, gravedad, impacto e IoC en un máximo de 72h - *Los OIV tienen un plazo de 24h donde se les pedirá el plan de acción.*
- 15 días corridos para entregar el informe final.

El reporte de incidentes de ciberseguridad, debe seguir un formato XML específico, clasificando la severidad de los incidentes y utilizando la taxonomía de ANCI y asegurar la trazabilidad de las actualizaciones realizadas en el reporte.

Conoce más:
Decreto N° 295: Reglamento de reportes de incidentes de ciberseguridad

Auditorías, análisis de riesgos y simulacros

OSE : ✗ **OIV:** ✓

La normativa obliga a realizar auditorías internas y externas, evaluaciones de riesgos periódicas y simulacros de ciberseguridad. Estas actividades buscan probar la efectividad de los controles implementados y asegurar que las organizaciones estén listas para responder ante incidentes reales sin improvisación.

Elaborar e implementar planes de continuidad operacional y ciberseguridad

OSE : ✗ **OIV:** ✓

Las organizaciones deben contar con planes de continuidad operacional y ciberseguridad certificados según el artículo 28 de la ley. Estos planes permiten mantener servicios críticos durante y después de un incidente. Además, deben revisarse al menos cada dos años para garantizar su vigencia y efectividad.

Recomendamos:
Crea tu plan de respuesta a incidentes de ciberseguridad

Elaborar e implementar planes de continuidad operacional y ciberseguridad

OSE : ✗ **OIV:** ✓

Las organizaciones deben contar con planes de continuidad operacional y ciberseguridad certificados según el artículo 28 de la ley. Estos planes permiten mantener servicios críticos durante y después de un incidente. Además, deben revisarse al menos cada dos años para garantizar su vigencia y efectividad.

Recomendamos:
Crea tu plan de respuesta a incidentes de ciberseguridad

Adoptar medidas para reducir el impacto y la propagación de incidentes

OSE : ✗ **OIV:** ✓

Ante un incidente de ciberseguridad, los OIV están obligados a actuar con rapidez para mitigar el daño. Esto incluye medidas como restringir el acceso a sistemas, desconectar redes comprometidas o aislar equipos afectados para evitar una propagación mayor.

Contar con certificaciones según el artículo 28

OSE : ✗ **OIV:** ✓

Para los OIV, la ley exige que las organizaciones obtengan certificaciones (ej: ISO 27001) que acrediten la efectividad de su SGSI y sus planes de continuidad. Esto sirve como respaldo frente a la ANCI y demuestra que los procesos cumplen con estándares reconocidos.

Para el caso particular de los OSE, no se obligará a presentar una certificación, no obstante, la reglamentación técnica de ANCI se basará en controles técnicos de estándares y normativas internacionales (ISO 27001, NIST, CIS, etc).

Notificación a potenciales afectados

OSE : ✗ **OIV:** ✓

Cuando un ciberataque comprometa datos o sistemas críticos, las organizaciones deben informar a las personas potencialmente afectadas, siempre que puedan ser identificadas y la ANCI así lo requiera. Esto es especialmente importante cuando se involucran datos personales o existe riesgo de nuevos incidentes.

Programas de capacitación y campañas de ciberhigiene

OSE : ✗ **OIV:** ✓

La formación continua es clave para fortalecer la cultura de seguridad. Los OSE y OIV deben implementar programas de capacitación para trabajadores y colaboradores, con campañas regulares de ciberhigiene que promuevan buenas prácticas y reduzcan el riesgo de errores humanos.

Cumplimiento de normativas técnicas ANCI o sectoriales

OSE : ✓ **OIV:** ✓

Además de las obligaciones generales dadas por ANCI, las organizaciones deben adherirse a los estándares técnicos que dicte la ANCI o su regulador sectorial (CMF, SiSS, SEC,SuperSalud, SUBTEL, Coordinador Eléctrico Nacional). Esto garantiza que sus medidas de ciberseguridad estén alineadas con las mejores prácticas nacionales e internacionales, adaptadas a las características de su industria.

Descargar nuestro checklist de cumplimiento de la ley Marco
Descubre cómo simplificar el cumplimiento paso a paso sin complicaciones técnicas.

04

Qué pasa si no cumples

Qué pasa si no cumples

La Ley marco clasifica las infracciones en tres niveles: leves, graves y gravísimas. Cada categoría depende de la naturaleza y el impacto del incumplimiento. Las leves incluyen retrasos en la entrega de información no crítica; las graves abarcan la falta de implementación de estándares o la omisión de reportes obligatorios; y las gravísimas son las más severas, asociadas a incidentes de alto impacto o reincidencias.

Tipo de infracción	Definición breve	Multa máxima (OSE)	Multa máxima (OIV)
Leve	Retrasos en reportes no críticos o incumplimientos menores.	5.000 UTM	10.000 UTM
Grave	No implementar estándares, omisión de reportes críticos, obstaculización.	10.000 UTM	20.000 UTM
Gravísima	Reincidencia en infracciones graves o incidentes con impacto significativo.	20.000 UTM	40.000 UTM

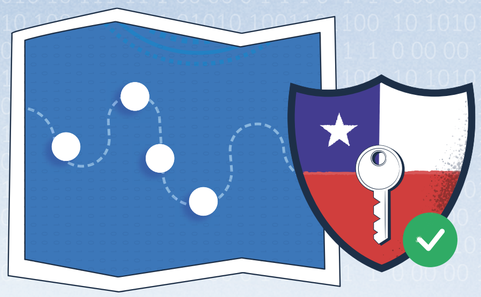
Tipos de infracciones según el artículo 38

Categoría Infracciones	Infracciones OSE	Infracciones OIV
Infracciones Leves	• Entregar fuera de plazo la información solicitada, siempre que no sea crítica para la gestión de un incidente. • Incumplir instrucciones de la ANCI cuando no constituyan una infracción grave o gravísima. • Cualquier otra infracción sin sanción especial definida en la ley.	• No mantener el registro de las acciones de seguridad realizadas. • No comunicar al CSIRT Nacional sobre revisiones y ejercicios continuos. • No implementar programas de capacitación y educación continua en ciberseguridad. • No designar un delegado de ciberseguridad. • Incumplir con la certificación de planes de continuidad operacional. • No contar con las certificaciones exigidas por la ley.
Infracciones Graves	• No implementar los protocolos y estándares de la ANCI para gestionar ciberincidentes. • No aplicar los estándares sectoriales de ciberseguridad. • Entregar fuera de plazo información necesaria para gestionar un incidente. • Presentar información falsa o errónea a la ANCI. • Omitir el reporte obligatorio de incidentes (artículo 9°). • Negarse sin justificación a cumplir instrucciones o entorpecer la labor de la ANCI durante un incidente. • Reincidir en una infracción leve dentro de un año.	• No implementar un SGSI continuo. • No elaborar ni ejecutar los planes de continuidad operacional y ciberseguridad. • No informar a los afectados sobre incidentes que comprometan datos críticos. • No tomar medidas rápidas para contener y reducir el impacto de un incidente o ciberataque. • Reincidir en una infracción leve dentro de un año.
Infracciones Gravísimas	• Entregar información falsa o errónea a la ANCI cuando sea crucial para la gestión de un incidente significativo. • Desobedecer instrucciones de la ANCI durante un incidente de alto impacto. • Negarse a entregar información esencial para incidentes significativos. • Reincidir en una infracción grave dentro de un año.	• No aplicar medidas de contención en incidentes de impacto significativo. • Reincidir en una infracción grave dentro de un año.

Los factores agravantes pueden elevar las sanciones impuestas. La reincidencia, el impacto económico o social del incumplimiento y el tamaño de la empresa son elementos que la ANCI considera al determinar la multa. Las organizaciones de mayor relevancia estratégica enfrentan sanciones más altas si no toman medidas para mitigar riesgos.

Por ejemplo, un OIV que no informa un ciberataque a potenciales afectados comete una infracción grave. Si además no toma acciones para contener la amenaza y el incidente afecta servicios esenciales, la falta puede escalar a gravísima, con multas millonarias y posibles inhabilitaciones operativas.

05



Pasos prácticos para cumplir con la Ley 21.663

Pasos prácticos para cumplir con la Ley 21.663

En esta sección encontrarás un punto de partida claro: una hoja de ruta con los pasos clave para implementar un SGSI, adoptar las herramientas correctas y preparar a tu equipo para los retos de la Ley 21.663. Sigue esta guía para avanzar con confianza y asegúrate de que tu organización esté lista para lo que viene. ¿Listo para ponerte manos a la obra?

Diagnóstico inicial

Antes de lanzarte a implementar controles o comprar soluciones de seguridad, necesitas saber dónde estás parado. El diagnóstico inicial es como un chequeo general para tu organización: identifica activos críticos, evalúa riesgos y detecta brechas en tus procesos actuales. Este paso te da una visión completa de tus puntos fuertes y áreas que necesitan atención para cumplir con la Ley 21.663.

Pasos del diagnóstico inicial:

Inventario de activos: Haz un inventario completo de todos los activos de información: dispositivos físicos como laptops y servidores, sistemas operativos, redes, aplicaciones y datos sensibles. Este paso es clave para saber qué necesitas proteger y para identificar qué tan expuesto está tu entorno actual a posibles amenazas.

Análisis de riesgos: Realiza un análisis detallado de las amenazas que podrían afectar tu operación, considerando vulnerabilidades internas y externas. Evalúa la probabilidad de que ocurran incidentes y el impacto que tendrían sobre tus servicios esenciales, usuarios y reputación. Esta información te ayudará a priorizar las acciones de seguridad más críticas.

Revisión de políticas actuales: Examina si ya existen políticas o procedimientos relacionados con la seguridad de la información. Pregúntate: ¿cubren realmente los riesgos actuales? ¿Están alineadas con estándares como ISO 27001? Este análisis permite identificar vacíos normativos y ajustar la gobernanza antes de implementar un SGSI.

Mapeo de procesos: Identifica cómo se mueve la información dentro de la organización: quién accede a qué datos, cómo se comparten y dónde podrían existir puntos débiles. El objetivo es visualizar el flujo de trabajo y encontrar procesos que requieran controles adicionales para proteger la integridad y confidencialidad de los datos.

Reporte de brechas: Elabora un informe claro con las brechas y vulnerabilidades detectadas en los pasos anteriores. Prioriza las áreas críticas según su riesgo e impacto potencial. Este documento servirá como base para tu plan de acción y te permitirá demostrar a la dirección la necesidad de invertir en seguridad.

Recursos adicionales:

- Cómo implementar un programa de gestión de riesgos
- Matriz de riesgos: Guía para lideres de TI

Designación del responsable

Una vez que sabes dónde estás, es hora de nombrar a la persona que liderará el cambio. La ley pide un delegado de ciberseguridad como enlace con la ANCI, pero en organizaciones grandes se recomienda sumar un equipo de apoyo para que el delegado no cargue solo con toda la gestión y notificación de incidentes. Este rol será clave para coordinar acciones, monitorear avances y garantizar que el SGSI se mantenga vivo y actualizado.

Evaluación y selección de un marco SGSI (ISO/NIST)

Elegir un marco de referencia sólido es un paso crucial para estructurar tu SGSI y cumplir con la Ley 21.663. Aunque existen varios, como NIST CSF, recomendamos ISO 27001, ya que es el estándar en el que se basa la normativa chilena. Además, facilita auditorías y certificaciones internacionales. NIST puede ser un buen complemento para organizaciones con operaciones en EE. UU. o entornos muy técnicos.

Aspecto	ISO 27001	NIST Cybersecurity Framework
Enfoque	Sistema de gestión completo basado en ciclo PDCA (Plan-Do-Check-Act).	Marco de buenas prácticas y controles flexibles para gestión de riesgos.
Certificación	Certificable a nivel internacional.	No certificable, es una guía voluntaria.
Alineación con Ley 21.663	Totalmente alineado, la ley lo menciona como referencia principal.	Puede complementar, pero no reemplaza ISO.
Cobertura geográfica	Reconocido globalmente, útil para operaciones internacionales.	Muy usado en EE. UU. y sectores técnicos.
Uso ideal	Organizaciones que buscan un SGSI estructurado y certificable.	Entidades que necesitan guías prácticas rápidas y flexibles.

Automatización de alertas y trazabilidad

Cuando hablamos de ciberseguridad, el tiempo de reacción lo es todo. Automatizar alertas te permite detectar y responder a incidentes en tiempo real, sin depender de que alguien “se dé cuenta a tiempo”. Por otro lado, la trazabilidad no es opcional: la Ley 21.663 exige registros detallados para demostrar acciones y decisiones en auditorías. Ambas cosas juntas te dan control y tranquilidad.

Elemento	¿Qué es?	¿Qué ofrece?	¿Qué aporta?	Cómo y con qué app
Automatización de alerta	Un sistema que genera notificaciones automáticas cuando detecta comportamientos anómalos o incidentes, como accesos no autorizados o cambios en configuraciones críticas.	Alertas en tiempo real por email, SMS o dashboards, para que tu equipo pueda reaccionar rápido.	Reduce tiempos de respuesta y mitiga el impacto de ataques antes de que escalen.	Herramientas tipo SIEM para alertas basadas en logs de eventos complejos. Con Prey, puedes configurar reglas automáticas (geofencing, batería baja, cambios de hardware) para recibir notificaciones instantáneas y aplicar acciones remotas como bloqueo o borrado.
Trazabilidad	El registro continuo y detallado de todas las actividades y eventos relacionados con la seguridad de la información.	Logs de auditoría completos con fechas, responsables y acciones tomadas, cumpliendo con los requisitos de la Ley 21.663.	Facilita auditorías y demostraciones de cumplimiento, además de ayudar a reconstruir la cadena de eventos tras un incidente.	Exigir módulos de reportería a soluciones contratadas. Plataformas como Vanta o Drata para centralizar logs y generar reportes automáticos de cumplimiento. Prey mantiene un historial de acciones ejecutadas (bloqueos, recuperaciones, cambios de configuración) para aportar evidencia clara en auditorías.

Capacitación y concientización interna

Puedes tener el mejor firewall del mundo, pero si alguien en tu equipo abre un archivo adjunto sospechoso, el castillo se viene abajo. La formación continua no es opcional: es tu mejor defensa contra errores humanos, que el DBIR 2025 identifica como causa en el 60% de las brechas. Un equipo bien entrenado es un escudo activo contra amenazas.

Ideas y plataformas para capacitar a tu equipo

- **Simulaciones de phishing**
  Crea campañas falsas de phishing para entrenar al personal en la detección de correos fraudulentos.

  Plataforma recomendada: KnowBe4, Proofpoint Security Awareness.

- **Cursos interactivos de ciberseguridad**
  Ofrece módulos cortos y dinámicos sobre prácticas de higiene digital, uso seguro de contraseñas y manejo de datos sensibles.

  Plataforma recomendada: Udemy for Business, Coursera.

- **Cartelería digital y recordatorios**
  Usa screensavers, emails o apps internas para reforzar mensajes clave (no compartir contraseñas, cuidado con USB desconocidos, etc.).

  Plataforma recomendada: herramientas internas de comunicación como Slack.

- **Simulacros de incidentes**
  Realiza ejercicios prácticos donde los equipos respondan a un ciberataque simulado, desde el reporte hasta la contención.

  Plataforma recomendada: Cyberbit, RangeForce.

Define tu plan de continuidad operativa (PCO) y respuesta ante incidentes

Cuando algo falla —y tarde o temprano lo hará— lo importante no es solo evitarlo, sino saber cómo reaccionar. La Ley 21.663 exige a las organizaciones tener un PCO para garantizar que los servicios esenciales sigan funcionando tras un ciberataque. Aquí te conviene mirar el ISO 22301, el estándar de referencia en continuidad de negocio.

¿Qué involucra un PCO y un plan de respuesta ante incidentes

- **Identificación de procesos críticos:** Define qué operaciones no pueden detenerse bajo ninguna circunstancia y los recursos necesarios para mantenerlas activas.
- **Evaluación de riesgos y análisis de impacto:** Analiza escenarios de fallas y su efecto en los servicios, priorizando áreas que requieren planes robustos.
- **Protocolos de respuesta rápida:** Establece pasos claros para contener, mitigar y notificar incidentes (incluyendo reportes a la ANCI en menos de 3 horas).
- **Roles y responsabilidades:** Asigna quién hace qué durante una crisis, desde el equipo técnico hasta la alta dirección.
- **Pruebas y simulacros periódicos:** Ensaya los planes con regularidad para asegurarte de que realmente funcionen cuando los necesites.
- **Planes de recuperación y retorno a la normalidad:** Diseña cómo restaurar los servicios y sistemas a pleno rendimiento tras la contención del incidente.
- **Etapa de lecciones aprendidas y re-evaluación:** Una vez un incidente de seguridad se haya solucionado, se debe hacer un estudio de lecciones aprendidas para revisar qué salió mal y qué se puede mejorar para evitar repetir y tener mejores tiempos de respuestas ante dicho incidente.

Pruebas, simulacros y auditorías

Tener un plan suena bien, pero ¿funciona cuando las cosas se ponen feas? Las pruebas, simulacros y auditorías son la única forma de asegurarte de que tus controles y procesos no fallarán cuando realmente los necesites. Además, la Ley 21.663 exige revisiones periódicas, mínimo cada dos años, para mantener todo afinado y listo.

Elemento	¿Qué es?	¿Qué aporta?	¿Qué involucra?
Pruebas	Ejecuciones controladas de sistemas y procesos para comprobar su correcto funcionamiento.	Permite identificar fallos técnicos o de configuración antes de un incidente real.	Revisar backups, verificar que alertas se disparen correctamente, probar acceso a sistemas tras un fallo simulado.
Simulacros	Ejercicios prácticos en los que se simula un incidente de seguridad para evaluar la respuesta del equipo.	Entrena al personal y pone a prueba la coordinación y la toma de decisiones bajo presión.	Escenarios como ataques de ransomware o pérdida masiva de datos; roles definidos y tiempos cronometrados.
Auditorías	Evaluaciones formales y periódicas para revisar el cumplimiento de políticas y normativas de seguridad.	Ofrece evidencia documentada para la ANCI y asegura alineación con estándares como ISO 27001 o 22301.	Escenarios como ataques de ransomware o pérdida masiva de datos; roles definidos y tiempos cronometrados.

Plan de implementación por fases

Intentar implementar un SGSI de golpe puede ser abrumador, costoso y poco realista. Por eso recomendamos dividirlo en fases pequeñas mas manejable en el tiempo. Este enfoque permite priorizar lo más crítico, gestionar recursos de forma eficiente y mostrar avances rápidos a la dirección. Además, facilita ajustes antes de una implementación total.

Aquí te damos un ejemplo de implementación por fases:

Fases	Nombre	Descripción
Fase 1	Diagnóstico y planificación	Realizar el diagnóstico inicial y definir el alcance del SGSI.
Fase 2	Políticas y procedimientos básicos	Redactar políticas de seguridad y establecer roles y responsabilidades.
Fase 3	Controles técnicos iniciales	Implementar medidas clave como control de accesos y backups.
Fase 4	Formación y concientización	Capacitar a los equipos en buenas prácticas de ciberseguridad.
Fase 5	Auditorías internas y ajustes	Probar el sistema, identificar brechas y hacer correcciones antes de la certificación o auditoría.

Documentación y evidencia

En ciberseguridad, lo que no está documentado “no existe” a los ojos de un auditor. La Ley 21.663 exige mantener registros claros y actualizados para demostrar que realmente aplicas las medidas de seguridad. Esta evidencia no solo es útil para cumplir, también te salva cuando necesitas reconstruir lo que pasó tras un incidente.

Documentación clave que deberías tener a mano

- **Políticas y procedimientos**
  - Política de seguridad de la información.
  - Procedimientos de gestión de incidentes.
  - Planes de continuidad operativa y recuperación de desastres.
- **Registros de actividades**
  - Logs de acceso a sistemas críticos.
  - Historial de configuraciones y cambios en la infraestructura.
  - Ejecuciones de acciones remotas (como bloqueos o borrados con Prey).
- **Evidencia de capacitación**
  - Listados de sesiones de formación realizadas.
  - Certificados de participación del personal.
  - Resultados de campañas de concientización (simulaciones de phishing, por ejemplo).
- **Informes de auditorías y simulacros**
  - Auditorías internas y externas completas.
  - Resultados y lecciones aprendidas de simulacros de ciberataques.
  - Planes de acción derivados de las auditorías.
- **Certificaciones y cumplimiento**
  - Certificados ISO 27001 o ISO 22301 (si los tienes).
  - Evidencia de revisiones periódicas según la Ley 21.663.
  - Reportes enviados a la ANCI o al CSIRT Nacional.
- **Inventario de dispositivos y quienes lo manejan**
  - Laptops y desktops corporativos.
  - Dispositivos móviles (smartphones y tablets).
  - Servidores locales y en la nube.
  - Equipos de red (routers, switches, firewalls físicos).
  - Dispositivos IoT críticos (cámaras de seguridad, sensores, etc.).
  - Medios de almacenamiento externo (discos duros, USBs, backups físicos).

Herramientas tecnológicas recomendadas

Hoy en día, pensar que basta con un antivirus y una VPN es como creer que con cerrar la puerta de tu casa basta para detener a un ladrón con llave maestra. Ya sea en oficinas o entornos remotos, todos llevamos un pedazo del trabajo a casa (sí, ese portátil con datos críticos o el móvil con acceso al correo de trabajo). Por eso necesitas un stack de seguridad que realmente cubra todos los frentes.

En esta lista no solo te mostraremos las herramientas clave que no pueden faltar, sino también datos recientes del Data Breach Investigation Report 2025 que demuestran por qué son tan importantes para evitar quedar en las estadísticas de las próximas brechas:

Categoría	Descripción de la herramienta	Por qué importa	Ejemplos
MDM (monitoreo de dispositivos)	Monitorea laptops y móviles, aplica políticas, rastrea, bloquea o borra datos de forma remota desde una consola.	El 22% de las brechas arrancó por endpoints sin visibilidad ni control.	Prey , Microsoft Intune, Jamf Pro
Gestión de parches	Automatiza la distribución de actualizaciones de SO y aplicaciones, prioriza CVEs críticos y verifica su instalación.	20% de los incidentes explotó vulnerabilidades sin parchear.	Automox, ManageEngine Patch Manager Plus, Ivanti Neurons, WSUS
Protección de endpoints (AV + EDR)	El AV detiene malware conocido; el EDR monitoriza comportamientos, aísla hosts y orquesta respuesta en tiempo real.	44% de las brechas incluyeron ransomware.	Avast Business + CrowdStrike Falcon, SentinelOne
SIEM / UEBA	Centraliza logs, correla eventos y aplica analítica de comportamiento para destapar anomalías antes de que escalen.	60% de los ataques llevan factor humano.	Splunk, IBM QRadar, Microsoft Sentinel
Backups 3-2-1	Crea backups locales y en nube, prueba restauración y protege copias con inmutabilidad o air-gap.	Sin copias íntegras no hay rescate.	Veeam Backup & Replication, Acronis Cyber Protect
Gestor de contraseñas	Guarda contraseñas cifradas, genera claves fuertes	Credenciales robadas fueron la puerta en el 22% de los casos.	Bitwarden , 1Password, Keeper Security
IAM / CABS	Administra identidades, gestiona SSO y MFA, y aplica políticas de acceso granular basadas en rol o contexto.	Principio de mínimo privilegio: que cada Jedi use solo el sable que necesita.	Okta, Azure AD PIM, ForgeRock
Firewall perimetral / cloud	Filtra y segmenta tráfico, aplica reglas Zero Trust y detiene escaneos y exploits en tiempo real, aún en entornos híbridos.	Appliances y VPNs sin parches suman 22% de accesos iniciales.	Palo Alto Networks, Zscaler Zero Trust Exchange

Herramientas complementarias

Además del “stack básico” de seguridad, hay herramientas complementarias que llevan tu defensa al siguiente nivel. No son opcionales si quieres estar un paso adelante de las amenazas. Desde detectar intrusiones hasta educar a tu equipo, estas soluciones cierran brechas que los atacantes adoran explotar.

Categoría	Descripción de la herramienta	Qué cubre	Ejemplos
IDS/IPS	Monitoriza el tráfico de red, aplica firmas + heurística y, si es IPS, corta el ataque antes de que llegue al host.	Vulnerabilidades no parcheadas (+20% YoY) siguen circulando. IDS avisa; IPS bloquea.	Snort, Suricata, Cisco Secure IPS
Análisis de vulnerabilidades	Revisa hosts, apps y contenedores; correlaciona CVEs, puntúa riesgos y sugiere parches.	34% más exploits que el año pasado. Escanea antes de que lo haga el atacante.	Nessus Expert, Qualys VMDR, Rapid7 InsightVM
Concientización & phishing sim	Plataforma e-learning con módulos micro-learning, simulaciones de phishing y métricas de mejora.	El usuario sigue siendo el eslabón débil (60% de fallos). Entrena, prueba, repite.	KnowBe4, Whalemate, Hook Security, Phished
Automatización de compliance	Conecta logs, mapea controles (ISO 27001, NIST, ley 21 663) y produce reportes en un clic.	ANCI no espera excusas. Centraliza evidencias y genera reportes listos para auditoría.	Vanta, Hackmetrix, Drata, Tugboat Logic

Escenario realista para no morir en el intento.

1. **Define tu matriz de riesgo** y prioriza herramientas donde el impacto regulatorio sea mayor.
2. **Integra telemetría** (MDM → SIEM → SOAR) para correlacionar eventos y automatizar respuesta.
3. **Prueba tu plan B**: restaura un backup, simula un phishing, dispara un playbook de contención. la teoría sirve; la práctica salva tu lunes.

> Pro-tip: documenta todo el flujo. ANCI pedirá evidencias y tus futuros tú te lo agradecerán

06

Cómo Prey puede ayudarte a cumplir con la Ley 21.663

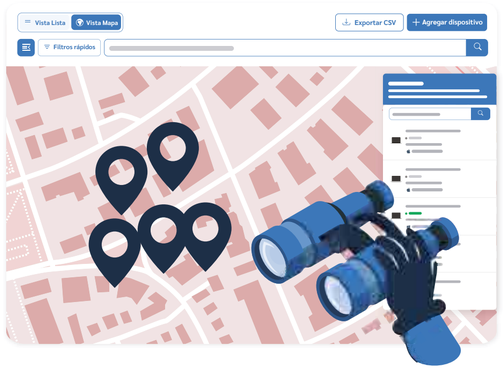
Cómo Prey puede ayudarte a cumplir con la Ley 21.663

Prey ofrece una solución práctica para organizaciones que buscan cumplir con los requisitos de la Ley 21.663 sin complicaciones. Su plataforma permite gestionar, proteger y monitorear dispositivos de forma centralizada, fortaleciendo el control sobre activos críticos, la reacción ante incidentes y la generación de evidencia para auditorías, todo desde una interfaz simple y accesible.

Detección de incidentes y reacción rápida

Con funciones como geofencing, alertas automáticas y detección de comportamientos inusuales, Prey permite identificar posibles incidentes en tiempo real. Además, puedes ejecutar acciones remotas como bloquear pantallas, activar alarmas y enviar mensajes, lo que agiliza la respuesta y reduce el impacto de un ciberataque o pérdida de equipo.

Visibilidad y control de tu flota

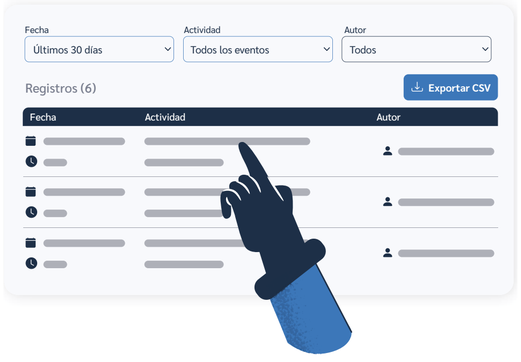


Prey te da una vista completa de todos los dispositivos en tu organización gracias a su panel centralizado. Puedes geolocalizar equipos, aplicar etiquetas y filtros personalizados, y gestionar múltiples sistemas operativos (Windows, macOS, ChromeOS, Android, Ubuntu) desde un solo lugar, facilitando la administración incluso en flotas grandes o dispersas.

Protección de datos en caso de pérdida o robo

Prey protege la información crítica de tus dispositivos con herramientas como Remote Wipe, Factory Reset y cifrado remoto con BitLocker en Windows. Estas funciones permiten borrar datos sensibles o inutilizar equipos robados para evitar accesos no autorizados y cumplir con las obligaciones de salvaguarda de datos exigidas por la ley.

Evidencia y trazabilidad para auditorías

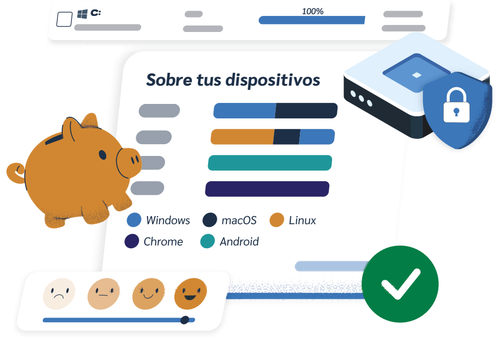


La plataforma mantiene un registro detallado de acciones y eventos gracias a su Audit Log. Esto incluye cambios en la configuración, movimientos de dispositivos y ejecuciones remotas, ofreciendo la trazabilidad necesaria para auditorías de la ANCI y demostrando el cumplimiento de protocolos de seguridad.

Monitoreo de brechas y credenciales en la Dark Web

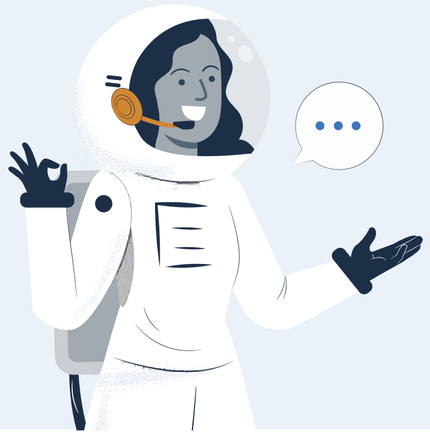
Prey también incluye un servicio de monitoreo en la Dark Web que detecta si las credenciales o datos de tu organización han sido filtrados. Esta función te permite tomar medidas preventivas, como el cambio inmediato de contraseñas comprometidas, evitando accesos no autorizados y cumpliendo con el deber de informar sobre incidentes críticos.

Apoyo para PYMEs y empresas con bajo presupuesto



Si tu organización aún no puede desplegar un SGSI completo como ISO 27001 o NIST, Prey es una alternativa multi-plataforma efectiva. Cubre controles clave como inventario, monitoreo, protección de endpoints, trazabilidad y respuesta rápida, todo desde una plataforma fácil de usar y sin sobredimensionar tu stack tecnológico o tus recursos.

¿Quieres ver cómo Prey puede ayudarte con el cumplimiento?



Si quieres conocer de primera mano cómo Prey puede fortalecer tu estrategia de ciberseguridad y apoyar el cumplimiento de la Ley 21.663, HIPAA, FERPA y otras normativas, te invitamos a solicitar una demo personalizada.

Solicita un demo guiada o escríbenos a sales@preyproject.com para conocer tu caso.

Sobre Prey

Es una herramienta multi-plataforma para el **Rastreo y la Seguridad** de tus dispositivos remotos. Es un servicio que actualmente protege más de 8 millones de equipos y sus datos cada día, alrededor de todo el mundo.

Prey comenzó en 2009 como una pequeña compañía de tecnología que se propuso un solo objetivo: ayudar a las personas a mantener el control de sus dispositivos. 15 años más tarde, nuestro servicio ha evolucionado hasta convertirse en una confiable multi herramienta para personas y negocios. Somos expertos en localizar, proteger y administrar tus dispositivos tecnológicos para el ocio y el trabajo. Y un equipo de personas orgullosas de poder ofrecerte apoyo.

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