daibackup

GUÍA DE CUMPLIMIENTO — 16 PÁGINAS

LEY 21.663: GUÍA PRÁCTICA DE CUMPLIMIENTO

Todo lo que tu empresa debe hacer para estar alineada

Obligaciones, plazos, controles técnicos y sanciones de la Ley Marco de Ciberseguridad en Chile — con checklist descargable y guía práctica por cada obligación.

EN ESTA GUÍA:

- Quién está obligado a cumplir
- Las 7 obligaciones clave, explicadas
- Plazos de reporte y multas
- Checklist técnico completo

CATEGORÍA
CIBERSEGURIDAD

VERSIÓN
v2.0 — Julio 2026

soporte@daibackup.cl | daibackup.cl

Índice

1 Contexto: qué es la Ley 21.663

La **Ley 21.663**, o **Ley Marco de Ciberseguridad**, es la primera normativa chilena que establece un marco legal obligatorio de gobernanza, gestión de riesgos y reporte de incidentes de ciberseguridad para organismos del Estado y operadores privados de servicios esenciales.

Fue publicada el 8 de abril de 2024 y sus artículos clave entraron en vigor el 1 de marzo de 2025. Crea dos instituciones centrales:

• **ANCI** (Agencia Nacional de Ciberseguridad) — el ente fiscalizador, encargado de calificar operadores, dictar resoluciones técnicas y aplicar sanciones.

• **CSIRT Nacional** — el canal oficial al que se deben reportar los incidentes de ciberseguridad dentro de los plazos que fija la ley.

Desde marzo de 2025 la ANCI ya está calificando operadores y el régimen de sanciones está activo: la conversación en las empresas chilenas pasó de "cuándo empezamos a evaluar esto" a "demuéstranos que ya estás al día". Si tu directorio pidió un estado de cumplimiento, o si tu área de TI opera en un sector regulado, este es el momento de tener el marco completo — no solo la parte técnica.

1/3

de los costos de una vulneración de datos se produce más de un año después del incidente.

22%

de esos costos se concentra específicamente durante el segundo año posterior al ataque.

Fuente: ENISA (estimación general de costos de brechas de datos)

Por qué importa hoy

La ANCI fiscaliza activamente desde marzo de 2025 y Chile registró múltiples ataques de ransomware a infraestructura crítica entre fines de 2025 y comienzos de 2026 — el marco dejó de ser teórico.

2 ¿Tu empresa está obligada a cumplir?

La ley distingue dos grandes grupos de afectados directos, aunque en la práctica sus efectos alcanzan a cualquier empresa que dependa de sus sistemas informáticos para operar — y en 2026, eso es prácticamente toda empresa.

Operadores de Importancia Vital (OIV)	Empresas calificadas formalmente por la ANCI por la criticidad de su operación para el país. Están sujetas al set completo de obligaciones: SGSI, reporte de incidentes, auditorías periódicas y controles técnicos verificables.
Prestadores de servicios esenciales	Energía, telecomunicaciones, agua, banca y servicios financieros, salud, transporte. Estos sectores concentran las obligaciones más exigentes de reporte y continuidad operacional.
Organismos del Estado	Ministerios, servicios públicos y municipalidades quedan sujetos a la misma institucionalidad de gobernanza y reporte que los operadores privados calificados.
El resto de las empresas (indirectamente)	Si eres proveedor, contratista o partner de un OIV, es muy probable que te exijan evidencia de buenas prácticas de seguridad como condición contractual — el estándar se propaga por la cadena de suministro.

Tip práctico: aunque no califiques como OIV, revisar este marco conviene igual — es el estándar que clientes, aseguradoras y directorios están empezando a exigir como buena práctica general.

Calificación como OIV

OBLIGACIÓN

01

EL PUNTO DE PARTIDA

Sin esto, no sabes qué tan estricta debe ser tu postura.

1 de 7

Determina si tu empresa califica como Operador de Importancia Vital o presta un servicio esencial. Es el primer paso: define qué tan exigente será el resto del cumplimiento.

■ Revisa si operas en energía, telecomunicaciones, agua, banca, salud o transporte — los sectores que la ley identifica como críticos.

■ Si no calificas directamente, revisa si eres proveedor de un OIV: la exigencia se propaga por la cadena de suministro contractualmente.

■ La calificación formal la realiza la ANCI mediante resolución — consulta a tu asesor legal si existe ambigüedad sobre tu categoría.

Primer paso práctico

Arma una lista simple de tus servicios (energía, agua, banca, salud, telecom, transporte) y compárala contra tu rubro real.
Si hay duda, una consulta corta con tu abogado corporativo zanja el tema antes de invertir en cualquier otro punto de esta guía.

Sistema de gestión (SGSI)

OBLIGACIÓN

02

EL CORAZÓN NORMATIVO

Es la evidencia que la ANCI revisa primero en una fiscalización.

2 de 7

Implementar un Sistema de Gestión de Seguridad de la Información conforme a los estándares mínimos que la ANCI ha ido precisando mediante resoluciones fundadas — no es un documento único, es un proceso vivo.

■ Define políticas de seguridad formales, aprobadas por la alta administración, no solo por el equipo técnico.

■ Documenta el inventario de activos críticos: sistemas, datos, proveedores y accesos.

■ Establece un ciclo de revisión periódica — el SGSI se audita y actualiza, no se archiva.

Primer paso práctico

Empieza por un inventario de activos críticos (sistemas, datos, proveedores) en una planilla simple — no necesitas software de SGSI para dar el primer paso. Define un responsable interno del SGSI, aunque sea a tiempo parcial: sin dueño, el sistema no se mantiene vivo.

Reporte de incidentes

Reportar todo incidente que pueda afectar la continuidad operacional o la confidencialidad, integridad y disponibilidad de los sistemas, dentro del plazo que fije la ANCI.

■ Define internamente qué constituye un "incidente reportable" antes de que ocurra uno — no lo decidas en caliente.

■ Ten un canal y responsable claro para reportar al CSIRT Nacional dentro del plazo exigido.

■ La omisión o el retardo constituye infracción grave — documenta cada paso del proceso de detección y reporte.

Primer paso práctico

Define hoy, por escrito, qué tipo de evento obliga a reportar y quién es el responsable de hacerlo.
Sin esta definición previa, cualquier incidente real se resuelve improvisando bajo presión, con más riesgo de error u omisión.

OBLIGACIÓN

03

EL MÁS SANCIONABLE

Ver sección de plazos y multas en la página 13.

3 de 7

Controles técnicos mínimos

OBLIGACIÓN

04

LO MÁS OPERATIVO

Es donde DaiBackup aporta más directamente (ver página 16).

4 de 7

La ley y sus resoluciones exigen un set de controles técnicos base, alineados con lo que ya es buena práctica internacional contra ransomware y accesos no autorizados.

■ MFA (autenticación de múltiples factores) obligatorio en accesos críticos y administrativos.

■ Segmentación de red para contener movimientos laterales de ransomware entre sistemas.

■ Cifrado de datos críticos tanto en reposo como en tránsito.

■ Backups inmutables — copias que ransomware no puede cifrar ni borrar.

Primer paso práctico

Prioriza MFA en los accesos administrativos esta semana — es el control con mejor relación costo/impacto para reducir compromisos de cuenta.
Súmale backups inmutables como segunda prioridad inmediata: cubre el escenario más probable de incidente, el ransomware.

Gestión de riesgos y continuidad

Más allá de prevenir, la ley exige poder seguir operando durante y después de un incidente: planes de respuesta y continuidad, no solo controles preventivos.

■ Plan de respuesta a incidentes documentado, con roles y responsables definidos de antemano.

■ Plan de continuidad de negocio: qué sistemas son críticos y cómo se recuperan primero.

■ Gap analysis o análisis de brechas periódico para priorizar quick wins de bajo costo.

Primer paso práctico

Identifica tus 3 a 5 sistemas realmente críticos y responde: ¿cuánto tiempo podemos estar sin ellos? Esa respuesta —no una lista genérica— define las prioridades reales de tu plan de continuidad de negocio.

OBLIGACIÓN

05

PREPARACIÓN, NO IMPROVISACIÓN

Un plan probado reduce drásticamente el tiempo de recuperación.

5 de 7

Gobernanza y deber de vigilancia

La ciberseguridad deja de ser un tema exclusivo de TI: el directorio y la alta administración asumen un deber de vigilancia explícito.

■ El directorio debe recibir reportes periódicos de postura de ciberseguridad, no solo enterarse tras un incidente.

■ La responsabilidad de vigilancia puede tener consecuencias legales para directores en caso de omisión grave.

■ Convierte la ciberseguridad en un punto fijo de la agenda de directorio, no en un informe anual aislado.

Primer paso práctico

Agenda ciberseguridad como punto fijo en la próxima reunión de directorio, aunque sea 10 minutos.
El hábito de reportar periódicamente importa más que el primer informe perfecto.

OBLIGACIÓN

06

EL CAMBIO CULTURAL

Muchas empresas chilenas ya cambiaron el tono de esta conversación.

6 de 7

Auditoría y evidencia

OBLIGACIÓN

07

LA PRUEBA DEL CUMPLIMIENTO

Sin evidencia, un buen control técnico no cuenta ante la ANCI.

7 de 7

No basta con implementar controles: hay que poder demostrarlos. La fiscalización de la ANCI se basa en evidencia documentada y verificable.

■ Valida tus controles con auditorías externas y pentesting periódico, no solo revisiones internas.

■ Mantén evidencia organizada y accesible: políticas, registros de incidentes, resultados de pruebas.

■ Trata la auditoría como una inversión, no un gasto — es lo que evita que un incidente técnico escale a crisis reputacional o legal.

Primer paso práctico

Antes de contratar una auditoría externa, ordena la evidencia que ya tienes: políticas, registros de incidentes, resultados de pruebas previas.
Un auditor avanza más rápido —y cobra menos— cuando encuentra orden previo en lugar de partir de cero.

3 Plazos de reporte y sanciones

La omisión o el retardo en el reporte de un incidente constituye una **infracción grave**. Distintas fuentes especializadas citan plazos de reporte de hasta 3 horas para las alertas iniciales ante la ANCI, y montos de multa que van desde 10.000 hasta 40.000 UTM según la gravedad de la infracción.

3 hrs

plazo citado para la alerta inicial de un incidente grave

40.000

UTM: multa máxima citada para infracciones gravísimas

Cifras citadas por fuentes especializadas en la Ley 21.663 — valida el detalle aplicable a tu categoría con tu asesor legal.

Gravedad	Ejemplo de causa	Consecuencia típica
Leve	Documentación incompleta o desactualizada	Requerimiento de subsanación
Grave	Retardo u omisión en el reporte de un incidente	Multa según categoría del operador
Gravísima	Daño significativo a infraestructura crítica	Multa máxima, posible duplicación

4 Ley 21.719: la ley complementaria de datos

La **Ley 21.719**, que crea la Agencia de Protección de Datos Personales, entra en vigencia el **1 de diciembre de 2026**. Obliga al responsable del tratamiento de datos a notificar las violaciones de seguridad que afecten datos personales a la autoridad y, en ciertos casos, a los titulares de esos datos.

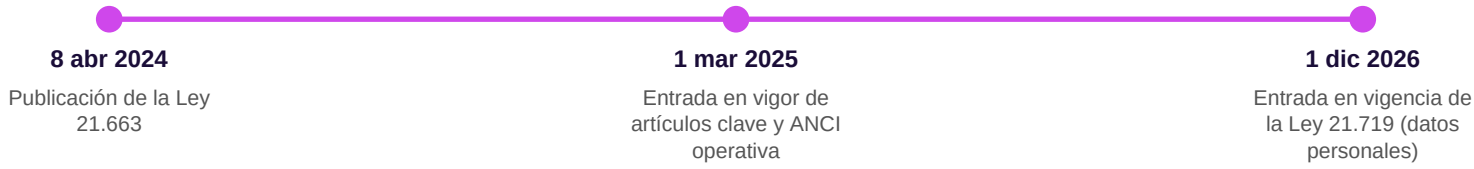
Ambas leyes son complementarias: muchas empresas —especialmente las que manejan datos de clientes, pacientes o colaboradores— deberán cumplir con las dos en paralelo.

Vale la pena abordar el cumplimiento de ciberseguridad (Ley 21.663) y de protección de datos (Ley 21.719) como un mismo proyecto: comparten gran parte de la infraestructura de controles, documentación y gobernanza.

Puntos en común entre ambas leyes

- Notificación de incidentes/violaciones dentro de plazos definidos.

Línea de tiempo



5 Checklist técnico completo

Marca cada punto ya cubierto en tu empresa. Úsalo como pauta de autoevaluación antes de una auditoría o fiscalización.

GESTIÓN DE ACCESOS

- ☐ MFA activo en todos los accesos administrativos y críticos
- ☐ Principio de mínimo privilegio aplicado en sistemas y datos
- ☐ Revisión periódica de accesos de ex-empleados y proveedores

RED Y ENDPOINTS

- ☐ Red segmentada para contener movimientos laterales
- ☐ Firewall de nivel empresarial, con filtrado avanzado
- ☐ EDR/antimalware centralizado en todos los servidores y equipos
- ☐ Parches de sistema operativo y aplicaciones al día

RESPALDO Y CONTINUIDAD

- ☐ Backups inmutables, no cifrables ni borrables por ransomware
- ☐ Regla 3-2-1 aplicada (3 copias, 2 medios, 1 fuera del sitio)
- ☐ Restauraciones probadas periódicamente, no solo el backup
- ☐ Plan de continuidad de negocio documentado

DATOS Y CIFRADO

- ☐ Cifrado de datos críticos en reposo y en tránsito
- ☐ Inventario de dónde residen los datos personales/sensibles

GOBERNANZA Y EVIDENCIA

- ☐ SGSI documentado y con revisión periódica
- ☐ Reportes de postura de ciberseguridad al directorio
- ☐ Auditorías externas o pentesting en el último año
- ☐ Proceso definido para reportar incidentes a la ANCI/CSIRT

Cómo DaiBackup apoya tu cumplimiento

Varias obligaciones técnicas de la Ley 21.663 —cifrado, continuidad operacional, resiliencia ante ransomware— se resuelven directamente con los servicios de DaiBackup.

DaiBackup Data Protection
BACKUP INMUTABLE

Copias que ransomware no puede cifrar ni borrar — clave para la continuidad operacional exigida por la ley y para restaurar sin pagar rescate.

DaiBackup M365 Backup
RESPALDO DE MICROSOFT 365

Respaldo de correo, OneDrive, SharePoint y Teams, protegiendo datos personales y corporativos alojados en la nube de Microsoft.

DaiBackup EDR
DETECCIÓN Y RESPUESTA

Detección y respuesta ante amenazas en endpoints, apoyando el control de riesgos y la trazabilidad exigida ante un incidente reportable.

Siguiente paso

Escríbenos a soporte@daibackup.cl para una revisión gratuita de tu postura de cumplimiento frente a la Ley 21.663, o visita daibackup.cl para conocer el detalle de cada servicio.

daibackup®

Protección de datos, continuidad operacional y cumplimiento.

DaiBackup ofrece backup inmutable, respaldo de Microsoft 365 y EDR para que tu empresa esté técnicamente alineada con la Ley 21.663 y resiliente ante ransomware.

soporte@daibackup.cl

daibackup.cl