

LEY DE PROTECCIÓN DE DATOS *en Chile*



*Del cumplimiento normativo a la
confianza digital*

Guía práctica para preparar tu
organización ante la **Ley 21.719** y fortalecer
la protección de los datos personales.

hiberus | Cybersecurity

El nuevo escenario: de la protección de datos en Chile

La transformación digital ha cambiado la forma en que las organizaciones gestionan la información.

Clientes, colaboradores, proveedores, usuarios y ciudadanos interactúan diariamente con múltiples plataformas y canales digitales. Como consecuencia, los datos personales se encuentran cada vez más distribuidos entre aplicaciones, servicios cloud, sistemas internos, proveedores y ecosistemas digitales.

Esta realidad aumenta las oportunidades para el negocio, pero también amplía la superficie de exposición.

Una vulneración de datos personales puede generar consecuencias que van mucho más allá del ámbito tecnológico: interrupciones operacionales, impactos económicos, pérdida de confianza, afectación reputacional y exposición regulatoria.

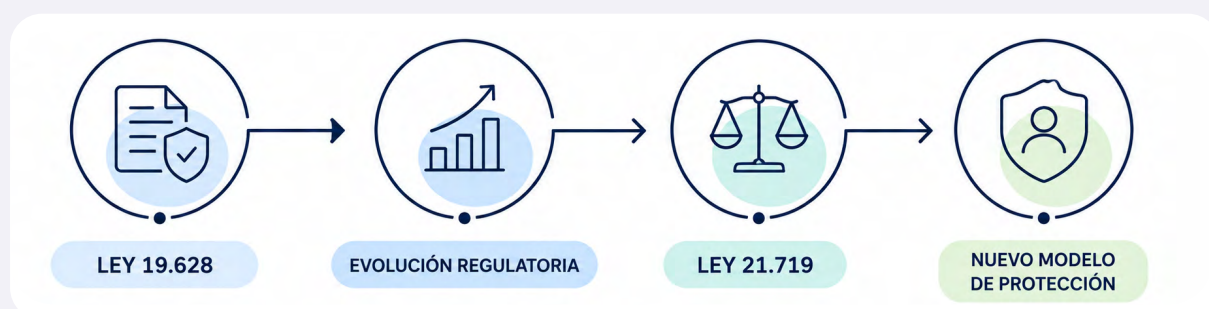
En este contexto, la Ley N.º 21.719 representa una evolución relevante del marco de protección de datos personales en Chile.

La normativa establece nuevos principios y obligaciones para quienes realizan tratamiento de datos personales, fortalece los derechos de los titulares y crea la Agencia de Protección de Datos Personales como autoridad encargada de fiscalizar y sancionar su cumplimiento.

La ley entra en vigor el 1 de diciembre de 2026.

El cumplimiento ya no debería entenderse únicamente como la existencia de políticas o documentos. Las organizaciones necesitan desarrollar la capacidad de demostrar que cuentan con medidas adecuadas para gestionar y proteger los datos personales que tratan.

La protección de datos deja de ser una responsabilidad exclusivamente legal y se convierte en un desafío transversal para toda la organización.



Las 5 claves de la nueva protección de datos



Responsabilidad demostrable

La organización debe ser capaz de acreditar que sus operaciones de tratamiento cumplen con la normativa y que existen medidas adecuadas para proteger los datos personales.



Mayor control para los titulares

Los titulares adquieren mayores capacidades para ejercer sus derechos y controlar el uso de su información personal.



Seguridad integrada en el tratamiento

La seguridad debe formar parte de la forma en que se diseñan y gestionan los procesos y sistemas que tratan datos personales.



Gobernanza y trazabilidad

Conocer qué datos se tratan, dónde están, quién accede a ellos y con qué finalidad se convierte en una capacidad fundamental.



Ciberseguridad y resiliencia

La protección de los datos requiere capacidades para prevenir, detectar, responder y recuperarse frente a incidentes de seguridad.



Clave 1. RESPONSABILIDAD DEMOSTRABLE

Cumplir también significa poder demostrarlo

La Ley 21.719 refuerza la responsabilidad de las organizaciones sobre los datos personales que tratan.

Esto implica no solo contar con políticas y procedimientos, sino poder demostrar que los tratamientos son adecuados y que existen medidas para proteger la información.



¿Qué debería conocer tu organización?

Qué datos trata

Qué información personal recopila y utiliza.

Para qué los trata

Cuál es la finalidad de cada tratamiento.

Dónde están

En qué sistemas, aplicaciones o entornos se encuentran.

Quién accede

Qué usuarios, áreas o terceros tienen acceso.

Cómo se protegen

Qué medidas técnicas y organizacionales existen.

*La pregunta ya no es solo si cumples, sino si puedes demostrar **cómo gestionas y proteges los datos.***

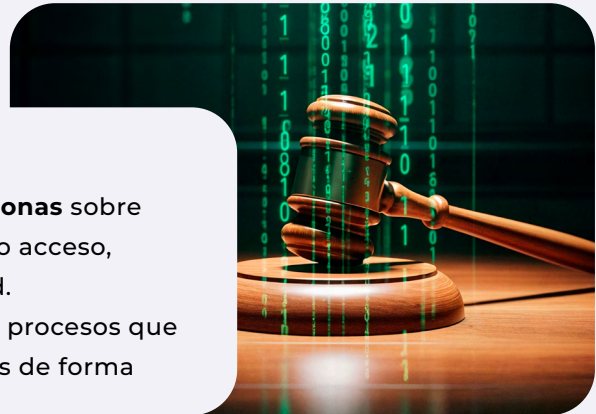


Clave 2. MÁS CONTROL PARA LOS TITULARES

El titular ocupa un lugar central

La Ley 21.719 fortalece los derechos de las personas sobre sus datos personales, incluyendo derechos como acceso, rectificación, supresión, oposición y portabilidad.

Para las organizaciones, esto implica contar con procesos que permitan gestionar y responder estas solicitudes de forma adecuada y trazable.



DE LA SOLICITUD A LA RESPUESTA



El desafío está en poder localizar la información personal cuando se encuentra distribuida entre múltiples sistemas, aplicaciones, plataformas cloud o proveedores. **Para responder a los titulares, primero hay que tener visibilidad sobre el dato.**

Clave 3. SEGURIDAD INTEGRADA EN EL TRATAMIENTO

Privacidad y ciberseguridad deben trabajar de forma coordinada

La protección de datos y la ciberseguridad están estrechamente relacionadas.

No basta con definir cómo se pueden utilizar los datos. También es necesario protegerlos frente a accesos no autorizados, pérdida, exposición o vulneraciones.



Dos capacidades, un mismo objetivo

Protección de datos

Gobernanza · Finalidad ·
Transparencia · Derechos

Ciberseguridad

Identidad · Accesos · Cloud · Aplicaciones
· Detección · Respuesta

El objetivo

Proteger la información y reducir el riesgo.

La seguridad debe incorporarse al ciclo de vida del dato y a los sistemas que lo procesan, desde su diseño hasta su eliminación.

Clave 4. GOBERNANZA Y RESILIENCIA

Conocer el dato para poder protegerlo

Para gestionar adecuadamente los datos personales, la organización necesita saber qué información trata, dónde se encuentra, quién accede a ella y con qué finalidad.

Un dato puede estar en muchos lugares

CRM · ERP · Cloud · SaaS · Aplicaciones · APIs · Sistemas legacy · Terceros



DE LA INFORMACIÓN AL CONTROL



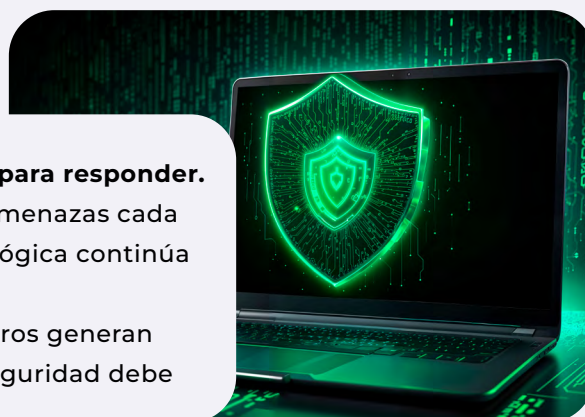
Esta trazabilidad permite pasar de un inventario estático a una visión real del riesgo asociado a la información personal. La protección de datos comienza por conocer el dato.

Clave 5. CIBERSEGURIDAD Y RESILIENCIA

El reto no es solo prevenir. Es estar preparado para responder.

Las organizaciones enfrentan un escenario de amenazas cada vez más dinámico, mientras su superficie tecnológica continúa creciendo.

Cloud, aplicaciones, APIs, trabajo remoto y terceros generan nuevos puntos de exposición. Por eso, la ciberseguridad debe abordar todo el ciclo de gestión del riesgo:



ANTICIPAR

Identificar riesgos y vulnerabilidades antes de que se conviertan en incidentes.



DETECTAR

Contar con visibilidad continua sobre amenazas y comportamientos anómalos.



RESPONDER

Actuar rápidamente para contener el incidente y reducir su impacto.



RECUPERAR

Restablecer la operación y mejorar las capacidades a partir de lo aprendido.

Seguridad + respuesta = resiliencia

La ciberseguridad deja de ser únicamente una función tecnológica y se convierte en una capacidad transversal para proteger la información, mantener la continuidad operacional y preservar la confianza.



DEL CUMPLIMIENTO A LA RESILIENCIA DIGITAL

Un mismo desafío: proteger el dato y el negocio

La adecuación a la Ley 21.719 no debería abordarse de forma aislada.

Protección de datos, ciberseguridad, gestión de riesgos y continuidad operacional forman parte de una misma estrategia.



El objetivo no es solo cumplir. Es construir una organización más preparada para gestionar el riesgo digital.

ROADMAP

¿Cómo preparar tu organización?

7 pasos para avanzar hacia el cumplimiento

02

Crear un proyecto de adecuación

01

Asignar responsables

03

Levantar el tratamiento de datos

04

Construir el catálogo de datos

05

Evaluar riesgos y brechas

06

Definir controles y políticas

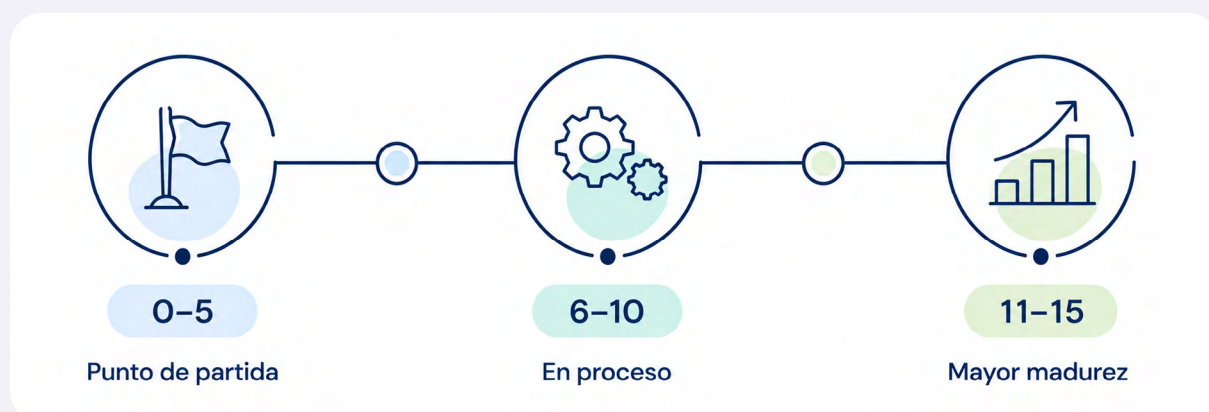
07

Implantar, medir y mejorar

Herramienta práctica: Checklist

¿Está preparada tu organización?

- ✓ Tenemos identificados los tratamientos de datos personales.
- ✓ Sabemos dónde están almacenados nuestros datos.
- ✓ Conocemos qué aplicaciones y sistemas los procesan.
- ✓ Tenemos identificados los terceros que acceden a información personal.
- ✓ Hemos definido responsables del programa de adecuación.
- ✓ Contamos con políticas actualizadas.
- ✓ Tenemos mecanismos para gestionar solicitudes de titulares.
- ✓ Revisamos periódicamente permisos y accesos.
- ✓ Contamos con controles de seguridad.
- ✓ Monitorizamos eventos de seguridad.
- ✓ Disponemos de procedimientos de respuesta ante incidentes.
- ✓ Hemos identificado los principales riesgos.
- ✓ Hemos evaluado las transferencias internacionales.
- ✓ Contamos con un roadmap de adecuación.
- ✓ Podemos demostrar las medidas implantadas.



hiberus CYBERSECURITY

Protección y resiliencia en un mundo digital sin perímetro

Ayudamos a las organizaciones a convertir la ciberseguridad en una capacidad continua de resiliencia, alineada con el negocio y preparada para un entorno digital cada vez más complejo.

Nuestras capacidades:

SOC SERVICES

Detección y respuesta 24x7

CNAPP

Seguridad cloud por diseño

ZERO TRUST

Confianza cero, control total

CIAM

La identidad como eje de la seguridad

CYBERAPP

Ciberseguridad desde el diseño

Algunos de los clientes de hiberus en el mundo que ya conocen y usan nuestras soluciones

Claro

CODORNÍU

CONSEJO GENERAL DE ENFERMERÍA

DKV

EDELVIVES

enel

HENNEO

HMY

iberCaja

MAPFRE

MAZ

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

natronale nederlanden

PRISA

Roca

Roche

santalucía
SEGUROS

Santander

Schindler

sesé

SICPA

hiberus

hiberus

La Ley 21.719 plantea un nuevo estándar para la protección de datos en Chile. Anticiparse es reducir riesgos, proteger la información y fortalecer la confianza.

En hiberus te ayudamos a convertir el cumplimiento en ciberseguridad y resiliencia digital.

Más información

