



VaultyX

MANUAL DE CUMPLIMIENTO PARA PYMES

Ley N° 21.719

Protección de Datos Personales en Chile

*De la exposición al control: una hoja de ruta clara,
gradual y aplicable a la realidad de tu empresa.*

VIGENCIA DE LA LEY: 1 DE DICIEMBRE DE 2026

Vaultyx · Protección de activos digitales para el mercado chileno · www.vaultyx.cl

Índice

Contenido

Índice	2
Antes de empezar	4
1. Los conceptos que sostienen toda la ley	5
1.1 ¿Qué cuenta como dato personal?	5
1.2 Datos sensibles: la categoría de máximo cuidado	5
1.3 ¿Cuándo se está "tratando" un dato?	6
1.4 Responsable, encargado y las figuras que se confunden	6
2. La base de licitud: el "por qué" detrás de cada dato	7
Consentimiento del titular	7
Ejecución de un contrato	7
Cumplimiento de una obligación legal	7
Interés legítimo	7
3. Transparencia: que nadie se entere después	8
Información mínima que el titular debe recibir	8
4. Seguridad: medidas proporcionales, no perfección	9
5. Los derechos ARSOP-B de los titulares	10
Cómo se gestiona una solicitud en la práctica	10
6. Proveedores: la cadena de terceros también es tu responsabilidad	11
Qué debe contener el acuerdo con un proveedor	11
7. Cuando algo sale mal: gestión de incidentes	12
Elementos mínimos de un procedimiento de respuesta	12
8. Responsabilidad demostrable: no basta con cumplir, hay que probarlo	13
Evidencia mínima recomendada	13
9. Una ruta de implementación en ocho etapas	14
Cronograma orientativo — junio a noviembre 2026	15
10. Autodiagnóstico rápido	16
Gobernanza	16
Inventario	16

Bases de licitud	16
Transparencia	16
Derechos ARSOP-B	16
Seguridad	16
Incidentes	16
Proveedores	16
Capacitación	17
Evidencia	17
Aviso legal	19

Antes de empezar

Este manual reúne, en un solo documento, lo que una pequeña o mediana empresa chilena necesita entender y ejecutar para adecuarse a la Ley N° 21.719, la norma que moderniza en profundidad el antiguo régimen de protección de datos personales de la Ley N° 19.628. No está pensado como un tratado jurídico, sino como una herramienta operativa: qué hacer, en qué orden, con qué evidencia y con qué plazos.

La ley entra en vigencia el 1 de diciembre de 2026. A partir de esa fecha, comenzará a operar además la Agencia de Protección de Datos Personales, el organismo que fiscalizará el cumplimiento y podrá imponer sanciones. Contar con un plan de adecuación no es opcional para ninguna organización que trate información de personas: clientes, trabajadores, proveedores o simples visitantes de un sitio web.

RIESGO REGULATORIO

Las multas contempladas por la Ley N° 21.719 se gradúan según la gravedad de la infracción: hasta 5.000 UTM en infracciones leves, hasta 10.000 UTM en infracciones graves y hasta 20.000 UTM en infracciones gravísimas. A esto se suman medidas correctivas, acciones judiciales de los propios titulares y, no menos importante, el daño reputacional frente a clientes y socios comerciales.

Este documento está organizado en tres bloques. El primero explica los conceptos y obligaciones centrales de la ley. El segundo propone una ruta de implementación en ocho etapas, pensada para que una PYME pueda avanzar con los recursos que realmente tiene disponibles. El tercero entrega herramientas de autoevaluación y respuestas a las dudas más frecuentes.

En Vaultyx acompañamos a empresas chilenas en cada una de estas etapas —desde el diagnóstico inicial hasta la implementación de controles técnicos, legales y de capacitación— con un enfoque de protección de datos y ciberseguridad integrado. Este manual es el punto de partida de ese proceso.

1. Los conceptos que sostienen toda la ley

Antes de construir cualquier política o procedimiento, conviene tener absoluta claridad sobre cuatro nociones que la Ley N° 21.719 utiliza constantemente: dato personal, dato sensible, tratamiento, y responsable/encargado. Si estos conceptos no quedan bien internalizados, es fácil subestimar el alcance real de la normativa.

1.1 ¿Qué cuenta como dato personal?

Un dato personal es cualquier antecedente que permite identificar a una persona natural, ya sea de forma directa (su nombre, su RUT) o indirecta, es decir, combinando distintos fragmentos de información que —juntos— apuntan a alguien en particular. Una dirección IP, un número de patente asociado a un conductor, o incluso un cargo laboral combinado con una ciudad pequeña pueden bastar para volver identificable a una persona.

Esta es la razón por la que casi ninguna empresa está exenta: basta con tener una planilla de clientes, un sistema de remuneraciones, cámaras de seguridad en la oficina o un formulario de contacto en el sitio web para estar tratando datos personales todos los días.

Categoría	Ejemplos habituales
Identificación	Nombre, RUT, fecha de nacimiento, nacionalidad
Contacto	Correo, teléfono, domicilio
Laboral	Cargo, sueldo, evaluaciones, asistencia
Comercial / financiero	Historial de compras, facturación, datos bancarios
Digital	IP, cookies identificables, geolocalización, huellas de navegación

En el extremo opuesto están los datos que la ley no protege: información agregada o estadística que ya no permite reconstruir a un individuo, y datos verdaderamente anonimizados —de forma irreversible— donde ya no existe forma razonable de volver a identificar al titular.

1.2 Datos sensibles: la categoría de máximo cuidado

Existe un grupo de datos que, por su naturaleza, exponen a las personas a riesgos de discriminación o afectan aspectos íntimos de su vida. La Ley N° 21.719 amplía considerablemente esta categoría respecto de la legislación anterior. Hoy se consideran sensibles, entre otros: el origen racial o étnico, las convicciones religiosas o filosóficas, las opiniones políticas, la afiliación sindical, los datos de salud, la orientación sexual, los datos biométricos, el perfil biológico y la situación socioeconómica.

PUNTO DE ATENCIÓN

Los datos biométricos merecen mención aparte: huella digital, reconocimiento facial y otros sistemas de autenticación biométrica quedan bajo un régimen reforzado, precisamente porque —a diferencia de una contraseña— no pueden "cambiarse" si son comprometidos.

La regla general para los datos sensibles es la prohibición: solo pueden tratarse si existe una autorización legal específica o un consentimiento explícito, libre, previo, específico e inequívoco del titular. Una casilla premarcada o un silencio del usuario no constituyen consentimiento válido bajo ningún escenario.

1.3 ¿Cuándo se está "tratando" un dato?

El tratamiento no se limita a guardar información en una base de datos. Cualquier operación —recolectar, ordenar, consultar, modificar, comunicar, respaldar, bloquear o eliminar— realizada sobre datos personales constituye tratamiento, sin importar si se hace de forma manual, en papel o mediante sistemas informáticos.

- Reclutamiento y gestión de personal.
- Videovigilancia y control de acceso a oficinas.
- Campañas de marketing y envío de correos comerciales.
- Formularios web, CRM y sistemas de facturación.
- Almacenamiento en plataformas cloud o aplicaciones móviles.

1.4 Responsable, encargado y las figuras que se confunden

La ley distingue con precisión tres situaciones que en la práctica suelen mezclarse: contratar un proveedor que procesa datos por instrucción de la empresa (encargado de tratamiento), entregar datos a un tercero que los usará para sus propios fines (cesión), y sacar información fuera de Chile (transferencia internacional). Cada una tiene requisitos distintos.

Figura	¿Quién define el fin del dato?	¿Requiere contrato?
Encargado de tratamiento	La empresa (Responsable)	Sí — DPA o cláusulas contractuales
Cesión de datos	El tercero receptor	Recomendable
Transferencia internacional	Depende del rol del receptor	Sí, en la mayoría de los casos

Antes de compartir datos con cualquier tercero —un proveedor de nube, una consultora, una plataforma SaaS extranjera— conviene hacerse cuatro preguntas simples: ¿el tercero sigue mis instrucciones o decide por sí mismo?, ¿existe un contrato que regule el tratamiento?, ¿los datos van a salir de Chile?, y ¿informé esto a los titulares? Las respuestas determinan qué figura aplica y qué obligaciones se activan.

2. La base de licitud: el "por qué" detrás de cada dato

Ningún dato personal puede tratarse simplemente porque la empresa lo considera útil. La Ley N° 21.719 exige que cada actividad de tratamiento se apoye en un fundamento legal concreto. En la práctica, para una PYME, las bases más relevantes son cuatro.

Consentimiento del titular

Debe ser una manifestación libre, específica, informada e inequívoca. El titular tiene que saber quién tratará sus datos, para qué y cómo puede revocar su autorización más adelante. Las casillas premarcadas y las fórmulas ambiguas no cumplen con el estándar.

Ejecución de un contrato

Cuando el tratamiento es indispensable para cumplir una relación contractual —emitir una factura, despachar un producto, gestionar un pago— no se requiere consentimiento adicional. El límite está en no usar esos mismos datos para fines ajenos al contrato sin una base adicional.

Cumplimiento de una obligación legal

Existen tratamientos que la propia ley impone o autoriza: cotizaciones previsionales, liquidaciones de sueldo, registros de asistencia, declaraciones tributarias o prevención de lavado de activos. Aquí el fundamento nace directamente de la norma sectorial correspondiente.

Interés legítimo

Permite tratar datos cuando existe un interés razonable de la empresa —seguridad de instalaciones, prevención de fraude, comunicaciones comerciales a clientes existentes— siempre que ese interés no prevalezca sobre los derechos del titular. Esta base exige un análisis previo, documentado, que pondere ambos intereses.

HERRAMIENTA CLAVE

Recomendación práctica: construye una Matriz de Tratamientos y Bases de Licitud. Es, probablemente, el documento más consultado durante una fiscalización, porque conecta cada actividad de la empresa con su fundamento legal específico.

3. Transparencia: que nadie se entere después

La ley parte de la base de que las personas tienen derecho a saber, desde el primer momento, qué se hace con su información. Esto se traduce en un deber de información que debe estar presente en cada punto de contacto donde se recolectan datos: sitios web, formularios, contratos y procesos de contratación laboral.

Información mínima que el titular debe recibir

- Quién es el responsable del tratamiento y cómo contactarlo.
- Para qué se usarán sus datos y bajo qué base de licitud.
- Si sus datos serán compartidos con terceros o transferidos fuera de Chile.
- Por cuánto tiempo se conservará la información.
- Qué derechos tiene (ARSOP-B) y cómo ejercerlos.

El vehículo principal para comunicar todo esto es la Política de Privacidad, que debe estar redactada en lenguaje claro —no solo jurídicamente correcto— y accesible en el sitio web o en el punto donde se recolectan los datos.

4. Seguridad: medidas proporcionales, no perfección

La normativa no exige una tecnología específica ni un presupuesto de nivel corporativo. Exige medidas razonables y proporcionales al riesgo real de cada organización. Para una PYME, esto normalmente se traduce en controles de tres tipos.

Tipo	Ejemplos
Organizacionales	Política interna, responsables definidos, capacitación, control de acceso
Técnicas	Contraseñas robustas, MFA, antivirus, respaldos periódicos, cifrado
Físicas	Control de acceso a oficinas, resguardo y destrucción segura de documentos

Es habitual que las PYMES chilenas convivan con vulnerabilidades silenciosas: planillas de clientes sin contraseña, credenciales compartidas entre varios colaboradores sin rotación, ausencia de respaldos externos automatizados, o dispositivos personales con acceso a información corporativa sin una política clara. Ninguna de estas brechas requiere una gran inversión para cerrarse, pero sí requiere que alguien las identifique primero.

5. Los derechos ARSOP-B de los titulares

La ley entrega a cada persona seis derechos concretos sobre su información, conocidos por el acrónimo ARSOP-B. Toda empresa debe estar preparada para recibir y responder estas solicitudes, incluso si nunca ha recibido una.

Derecho	En qué consiste
Acceso	Saber qué datos tiene la empresa, con qué fin y con quién los comparte
Rectificación	Corregir datos inexactos, incompletos o desactualizados
Supresión	Eliminar datos cuando ya no exista causa legal para conservarlos
Oposición	Frenar un tratamiento específico, por ejemplo publicidad o perfilamiento
Portabilidad	Obtener una copia estructurada de los datos para llevarlos a otro proveedor
Bloqueo	Suspender temporalmente el tratamiento mientras se resuelve un reclamo

Cómo se gestiona una solicitud en la práctica

Cada solicitud debería pasar por un flujo simple pero documentado: recepción por un canal identificado, verificación razonable de la identidad de quien solicita, análisis de procedencia, ejecución de la medida correspondiente, respuesta formal al titular y registro de todo lo anterior.

EVIDENCIA CLAVE

Un registro de solicitudes ARSOP-B —con fecha de recepción, derecho ejercido, responsable interno, análisis realizado y resultado— es una de las piezas de evidencia que la Agencia revisará con más atención durante una fiscalización.

6. Proveedores: la cadena de terceros también es tu responsabilidad

Prácticamente ninguna PYME opera sola: hay proveedores de nube, software de recursos humanos, plataformas de marketing, call centers, contadores externos. Cuando alguno de ellos procesa datos por cuenta de la empresa, se convierte en un Encargado de Tratamiento, y esa relación debe quedar regulada contractualmente.

Qué debe contener el acuerdo con un proveedor

- Objeto y duración del encargo, y finalidad autorizada del tratamiento.
- Tipo de datos y categorías de titulares involucrados.
- Medidas de seguridad exigidas al proveedor.
- Reglas de confidencialidad y de subcontratación.
- Procedimiento ante incidentes de seguridad.
- Devolución o eliminación de los datos al finalizar el servicio.

Cuando el proveedor almacena o procesa información fuera de Chile —algo frecuente con plataformas SaaS internacionales— se suma la exigencia de una transferencia internacional válida: un país con protección reconocida como adecuada, garantías contractuales equivalentes, consentimiento del titular en los casos que la ley prevé, u otra excepción legal aplicable.

ERROR FRECUENTE

Antes de contratar cualquier proveedor tecnológico, revisa si sus servidores están fuera de Chile. Es uno de los puntos que más sorprende a las PYMES durante un diagnóstico: muchas transferencias internacionales ocurren sin que nadie lo haya advertido.

7. Cuando algo sale mal: gestión de incidentes

Un incidente de seguridad puede ser un acceso no autorizado, la pérdida de un dispositivo, un envío de correo a la persona equivocada o un ataque informático. Lo relevante no es evitar que ocurra un cien por ciento del tiempo —eso es imposible— sino estar preparado para reaccionar rápido y de forma ordenada.

Elementos mínimos de un procedimiento de respuesta

- Un responsable designado para coordinar la respuesta.
- Un canal interno donde cualquier trabajador pueda reportar lo ocurrido.
- Un registro de incidentes, con fecha, alcance e impacto.
- Un criterio claro para decidir si corresponde notificar a la autoridad y a los titulares afectados.

PLAZO CRÍTICO

La ley exige notificar a la Agencia de Protección de Datos Personales dentro de un plazo de 72 horas desde que la empresa toma conocimiento de un incidente que pueda causar daño significativo a los titulares. Setenta y dos horas se agotan rápido si no existe un protocolo previo.

8. Responsabilidad demostrable: no basta con cumplir, hay que probarlo

La Ley N° 21.719 se construye sobre el principio de accountability: no es suficiente que la empresa efectivamente cumpla, debe poder demostrarlo con evidencia objetiva ante una fiscalización, un cliente o un tribunal. Esto cambia la forma en que hay que documentar el trabajo diario.

Evidencia mínima recomendada

- Inventario o Registro de Actividades de Tratamiento (RAT).
- Matriz de bases de licitud.
- Política de privacidad y política interna de protección de datos.
- Procedimientos de gestión ARSOP-B y de incidentes.
- Contratos y acuerdos de tratamiento con proveedores críticos (DPA).
- Registros de capacitación, solicitudes de titulares e incidentes.

La forma más simple de sostener todo esto en el tiempo es concentrar la evidencia en un repositorio único —una carpeta de cumplimiento— que cualquier responsable interno pueda actualizar y que esté disponible de inmediato si la empresa recibe un requerimiento.

9. Una ruta de implementación en ocho etapas

No hace falta abordar la Ley N° 21.719 como un proyecto monolítico. La siguiente ruta, pensada específicamente para la escala de una PYME, permite avanzar de forma ordenada, priorizando primero los riesgos más altos.

1. Designa un responsable

Nombra a la persona o equipo que coordinará el proceso. No necesita ser un área legal dedicada: puede ser gerencia, administración, RRHH o TI.

2. Levanta el inventario

Mapea todos los procesos donde se recopilan, usan o eliminan datos personales. Identifica sistemas, planillas y datos sensibles.

3. Asigna bases de licitud

Para cada tratamiento del inventario, define y documenta el fundamento legal que lo justifica.

4. Diagnostica brechas

Compara la situación real contra las exigencias legales. Clasifica cada hallazgo por nivel de riesgo (alto, medio, bajo).

5. Cierra las brechas prioritarias

Ejecuta acciones correctivas con responsable, plazo y recursos asignados, empezando por los riesgos altos.

6. Formaliza la documentación

Redacta o actualiza políticas, procedimientos y contratos: privacidad, seguridad, ARSOP-B, incidentes, DPA con proveedores.

7. Implementa controles y capacita

Pone en marcha las medidas de seguridad organizacionales, técnicas y físicas, y capacita a todo el equipo.

8. Revisa de forma continua

Audita periódicamente inventarios, contratos y procedimientos. La adecuación es un proceso permanente, no un proyecto que termina.

Cronograma orientativo — Septiembre a noviembre 2026

Un calendario razonable para llegar preparado a la entrada en vigencia del 1 de diciembre de 2026:

Actividad	Sep	Oct	Nov
Designación de responsable y autodiagnóstico	•		
Inventario de tratamientos	•		
Bases de licitud e informe de brechas	•		
Políticas de privacidad y protección de datos	•	•	
Procedimientos ARSOP-B e incidentes	•	•	•
Revisión de contratos y DPA con proveedores	•	•	
Medidas de seguridad y capacitación		•	•

10. Autodiagnóstico rápido

Antes de escribir la primera política, conviene tomarse veinte minutos para responder honestamente estas preguntas. No busca ser exhaustivo: busca revelar, de un vistazo, dónde están las prioridades.

Gobernanza

- ¿Hay una persona responsable de coordinar la protección de datos?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica
- ¿La dirección conoce las obligaciones de la Ley N° 21.719?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Inventario

- ¿Se sabe qué datos personales recopila la empresa y con qué fin?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica
- ¿Existe un registro de actividades de tratamiento?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Bases de licitud

- ¿Cada tratamiento tiene un fundamento legal identificado y documentado?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Transparencia

- ¿Existe una política de privacidad vigente y accesible?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Derechos ARSOP-B

- ¿Hay un canal y un procedimiento para gestionar solicitudes de titulares?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Seguridad

- ¿Existen contraseñas robustas, respaldos y control de acceso a los sistemas?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Incidentes

- ¿Existe un procedimiento para detectar, reportar y documentar incidentes?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Proveedores

- ¿Los contratos con proveedores regulan el tratamiento de datos personales?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Capacitación

- ¿El equipo ha recibido formación sobre protección de datos?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

Evidencia

- ¿Existe un repositorio con la documentación y registros de cumplimiento?
- ☐ Sí ☐ Parcial ☐ No ☐ No aplica

VAULTYX · DIAGNÓSTICO GRATUITO

¿Prefieres una evaluación guiada y con resultado inmediato? En www.vaultyx.cl puedes realizar el diagnóstico gratuito de Vaultyx y recibir una estimación de tu nivel de riesgo en minutos.



Siga el enlace [aquí](#)

O copie y pegue esta URL directamente en su navegador: [Diagnóstico de Cumplimiento Ley 21.719 | Vaultyx](#)

Preguntas Frecuentes

¿Toda empresa está obligada, sin importar su tamaño?

Sí. La ley aplica a cualquier organización, pública o privada, que trate datos de personas naturales chilenas, sin distinguir por tamaño ni facturación.

¿Siempre se necesita el consentimiento del titular?

No. El consentimiento es una entre varias bases de licitud. Muchos tratamientos se sostienen en la ejecución de un contrato, una obligación legal o un interés legítimo debidamente justificado.

¿Usar servicios en la nube está prohibido?

No está prohibido, pero la empresa sigue siendo responsable de verificar que el proveedor tenga medidas de seguridad adecuadas y de regular contractualmente esa relación.

¿Qué pasa si un cliente pide que eliminen sus datos?

Hay que evaluar si existe una obligación legal o contractual que justifique conservarlos. Si no la hay, corresponde eliminarlos o anonimizarlos.

¿Es obligatorio capacitar al equipo?

Sí. La capacitación es una de las medidas más efectivas para prevenir errores humanos, que son la causa más común de incidentes de seguridad.

¿Qué documentos mínimos debería tener una PYME?

Política de privacidad, política interna de protección de datos, procedimiento ARSOP-B, procedimiento de incidentes, registro de proveedores y evidencia de capacitación, como piso mínimo.

¿Qué significa 'responsabilidad demostrable'?

Que no basta con cumplir: la empresa debe poder probarlo con políticas, registros, contratos y evidencias concretas ante cualquier requerimiento.

¿Aún hay tiempo para prepararse?

Sí, pero el margen se reduce cada mes. Adecuarse implica revisar contratos, sistemas, proveedores y documentación interna, un proceso que rara vez se resuelve de un día para otro.

Aviso legal

Este manual tiene fines informativos y educativos. Ha sido elaborado por Vaultyx para apoyar a pequeñas y medianas empresas chilenas en su proceso de adecuación a la Ley N° 21.719, pero no constituye asesoría legal, auditoría de cumplimiento ni garantía de cumplimiento normativo. Tampoco reemplaza el análisis particular que cada organización debe realizar sobre sus propias actividades de tratamiento de datos.

La protección de datos personales es una materia en desarrollo permanente: la interpretación de distintos aspectos de la Ley N° 21.719 podrá precisarse mediante reglamentos, instrucciones de la Agencia de Protección de Datos Personales y jurisprudencia futura. Se recomienda revisar periódicamente la normativa vigente y buscar asesoría profesional especializada frente a tratamientos de alto riesgo, datos sensibles, transferencias internacionales o incidentes de seguridad.



Protección de activos digitales para el mercado chileno. Ciberseguridad, cumplimiento legal, auditoría IT y capacitación en un modelo de protección 360°.

www.vaultyx.cl · contacto@vaultyx.cl