etiqampus
e-Learning en Integridad

Protección de datos, guía esencial para pequeñas y medianas empresas

Marco Legal

NIVEL INTERMEDIO

Fecha	Año 2026
Tpo. de lectura	80 min.

La transformación digital ha permitido que empresas de todos los tamaños recopilen, almacenen y utilicen una cantidad cada vez mayor de información de clientes, trabajadores, proveedores y terceros.

En este contexto, la protección de los datos personales deja de ser una materia exclusiva de grandes compañías o áreas tecnológicas y pasa a convertirse en una obligación legal para toda organización que trate información vinculada a personas naturales.

La Ley N° 21.719, que entra en vigencia el 1° de diciembre del 2026, moderniza profundamente el régimen de protección de datos personales en Chile establecido originalmente en la Ley N° 19.628, creando un nuevo marco regulatorio basado en estándares internacionales de privacidad. La normativa contempla la creación de la Agencia de Protección de Datos Personales, organismo encargado de fiscalizar y sancionar los incumplimientos.

La protección de datos personales no debe entenderse únicamente como una obligación legal. También constituye una oportunidad para fortalecer la confianza de clientes, trabajadores y socios comerciales, mejorar la gestión de la información, reducir riesgos operacionales y diferenciarse competitivamente en un entorno donde la privacidad y la seguridad de los datos son cada vez más valoradas.

El plazo para prepararse ya comenzó. Las organizaciones que inicien tempranamente su proceso de adecuación podrán implementar las medidas de manera planificada y eficiente, evitando costos innecesarios y reduciendo significativamente los riesgos legales, reputacionales y económicos asociados al incumplimiento de la Ley N° 21.719.

El objetivo de este documento, elaborado por la Cámara de Comercio de Santiago, CCS, es entregar una metodología práctica, simple y proporcional para que las pequeñas y medianas empresas puedan implementar un Programa de Cumplimiento de manera gradual, ordenada y documentada, construyendo evidencia que les permita demostrar cumplimiento ante clientes, proveedores, trabajadores, autoridades y eventuales procesos de fiscalización.

FGE

CAMARA DE COMERCIO DE SANTIAGO

FUENTE: El texto de esta portadilla se elaboró a partir de extractos del documento que precede.

CÁMARA DE COMERCIO DE SANTIAGO

PROTECCIÓN DE DATOS

Guía Esencial para Pequeñas y Medianas Empresas

Herramientas prácticas para comprender las obligaciones legales, fortalecer el cumplimiento normativo y generar confianza en clientes y colaboradores.

N° 19.628 | **N° 21.719**

- Principios y obligaciones
- Derechos de los titulares
- Bases de licitud
- Medidas de seguridad
- Gestión de proveedores y terceros
- Buenas prácticas para PYMES
- Gestión de incidentes y brechas
- Estándares legales aplicables a empresas y organizaciones

CÁMARA DE COMERCIO DE SANTIAGO

2026

CÁMARA DE COMERCIO DE SANTIAGO

Programa de Cumplimiento PYME · Ley N° 19.628 modificada por la Ley N° 21.719

CONTENIDO

✓ **Ley N° 19.628 sobre Protección de Datos Personales, modificada por la Ley N° 21.719**

✓ Metodología proporcional y gradual diseñada para la realidad de las PYMES chilenas

✓ Entrada en vigencia de la Ley: 1 de diciembre de 2026

Introducción

La transformación digital ha permitido que empresas de todos los tamaños recopilen, almacenen y utilicen una cantidad cada vez mayor de información de clientes, trabajadores, proveedores y terceros. En este contexto, la protección de los datos personales deja de ser una materia exclusiva de grandes compañías o áreas tecnológicas y pasa a convertirse en una obligación legal para toda organización que trate información vinculada a personas naturales.

La Ley N° 21.719 moderniza profundamente el régimen de protección de datos personales en Chile establecido originalmente en la Ley N° 19.628, creando un nuevo marco regulatorio basado en estándares internacionales de privacidad. La normativa contempla la creación de la Agencia de Protección de Datos Personales, organismo encargado de fiscalizar y sancionar los incumplimientos.

⚠ La entrada en vigencia general de la Ley N° 21.719 está prevista para el 1 de diciembre de 2026.
✓ Ley N° 19.628 sobre Protección de Datos Personales, modificada por la Ley N° 21.719.

El objetivo de este documento es entregar una metodología práctica, simple y proporcional para que las pequeñas y medianas empresas puedan implementar un Programa de Cumplimiento de manera gradual, ordenada y documentada, construyendo evidencia que les permita demostrar cumplimiento ante clientes, proveedores, trabajadores, autoridades y eventuales procesos de fiscalización.

La metodología propuesta se estructura en etapas sucesivas que permiten a la organización avanzar desde el diagnóstico inicial hasta la implementación de políticas, procedimientos, registros y controles mínimos de cumplimiento. Cada etapa contiene actividades concretas, herramientas de apoyo y recomendaciones prácticas especialmente diseñadas para la realidad de las PYMES chilenas.

La protección de datos personales no debe entenderse únicamente como una obligación legal. También constituye una oportunidad para fortalecer la confianza de clientes, trabajadores y socios comerciales, mejorar la gestión de la información, reducir riesgos operacionales y diferenciarse competitivamente en un entorno donde la privacidad y la seguridad de los datos son cada vez más valoradas.

El plazo para prepararse ya comenzó. Las organizaciones que inicien tempranamente su proceso de adecuación podrán implementar las medidas de manera planificada y eficiente, evitando costos innecesarios y reduciendo significativamente los riesgos legales, reputacionales y económicos asociados al incumplimiento de la Ley N° 21.719.

El incumplimiento de la Ley N° 21.719 puede exponer a la empresa a procedimientos de fiscalización e investigación por parte de la Agencia de Protección de Datos Personales. En efecto, la ley contempla un sistema de infracciones y sanciones graduadas según su gravedad:

- **Infracciones leves:** multas de hasta **5.000 UTM**.
- **Infracciones graves:** multas de hasta **10.000 UTM**.
- **Infracciones gravísimas:** multas de hasta **20.000 UTM**.

Además de las multas, la Agencia podrá adoptar otras medidas correctivas, tales como ordenar la adecuación de procesos, instruir el cese de determinadas operaciones de tratamiento, exigir la implementación de medidas de seguridad o requerir la corrección de incumplimientos detectados.

Por su parte, los titulares de los datos personales podrán ejercer las acciones que contempla la ley ante los tribunales de justicia para solicitar la tutela de sus derechos, así como la indemnización de los perjuicios que acrediten haber sufrido como consecuencia de un tratamiento ilícito o incumplimiento de la normativa.

Adicionalmente, una infracción puede generar importantes consecuencias reputacionales, pérdida de confianza de clientes, trabajadores y proveedores, impactos comerciales y mayores costos de cumplimiento derivados de procedimientos administrativos o judiciales.

1. Principales Obligaciones bajo la Ley N° 21.719

La Ley N° 21.719 establece un modelo de cumplimiento basado en la responsabilidad proactiva o accountability. Esto significa que las organizaciones no solo deben cumplir con la normativa, sino también ser capaces de demostrar dicho cumplimiento mediante políticas, procedimientos, registros y evidencia objetiva.

1.1 Identificar los Tratamientos de Datos Personales

El primer paso consiste en conocer qué datos personales trata la organización, para qué fines los utiliza, dónde se almacenan, quiénes tienen acceso y con quiénes se comparten.

¿Qué son los Datos Personales?

Los datos personales son cualquier información vinculada o referida a una persona natural identificada o identificable.

Una persona se considera identificada cuando es posible determinar directamente quién es a partir de la información disponible. Por su parte, una persona es identificable cuando su identidad puede determinarse directa o indirectamente mediante uno o más datos o mediante la combinación de éstos con otra información razonablemente disponible. En consecuencia, el concepto de dato personal es amplio y no se limita únicamente al nombre o al RUT de una persona.

Ejemplos

Datos de identificación: nombre y apellidos, RUT, fecha de nacimiento, nacionalidad, estado civil.

Datos de contacto: dirección, correo electrónico, número telefónico, dirección postal.

Datos laborales: cargo, remuneración, historial laboral, evaluaciones de desempeño, registro de asistencia.

Datos comerciales y financieros: historial de compras, información de facturación, datos bancarios, información crediticia.

Datos tecnológicos: dirección IP, identificadores de dispositivos, cookies asociadas a una persona, geolocalización y registros de navegación cuando permitan identificar a una persona.

¿Cuales NO constituyen datos personales?

No constituyen datos personales aquellos antecedentes que no permiten identificar ni hacer identificable a una persona natural. Tampoco se consideran datos personales los datos que han sido debidamente anonimizados de forma irreversible, es decir, cuando ya no es posible identificar al titular utilizando medios razonables.

Ejemplos: estadísticas agregadas, información completamente anonimizada y datos puramente corporativos que no se vinculan a personas naturales.

Importancia para las PYMES. Muchas organizaciones creen que sólo tratan datos personales cuando almacenan nombres o RUT. Sin embargo, en la práctica, todas las empresas manejan datos personales en sus actividades cotidianas. Por ejemplo, una PYME trata datos personales cuando mantiene una base de clientes, gestiona trabajadores, contrata proveedores, utiliza formularios de contacto en su sitio web, envía correos electrónicos comerciales, opera sistemas de videovigilancia, utiliza plataformas de recursos humanos o CRM o gestiona procesos de selección de personal. Por ello, el primer paso para cumplir la Ley N° 21.719 consiste en identificar qué datos personales trata la organización, dónde se encuentran y para qué finalidades son utilizados.

¿Qué son los Datos Sensibles?

Los datos sensibles corresponden a una categoría especial de datos personales que, debido a su naturaleza, pueden afectar de manera significativa la privacidad, dignidad, derechos fundamentales o generar riesgos de discriminación para las personas. Por esta razón, la Ley N° 21.719 establece un régimen de protección reforzado para su tratamiento, imponiendo mayores exigencias respecto de las

bases de licitud, medidas de seguridad y responsabilidades de quienes los utilizan. En términos prácticos, mientras todos los datos personales se encuentran protegidos por la ley, los datos sensibles reciben una protección adicional debido al impacto que una divulgación, pérdida o uso indebido podría generar para sus titulares.

¿Qué Datos se Consideran Sensibles? La Ley N° 21.719 amplía significativamente la definición existente en la antigua Ley N° 19.628, incorporando nuevas categorías especialmente protegidas.

Entre los principales datos sensibles se encuentran: origen racial o étnico; convicciones religiosas, filosóficas o morales; opiniones o afiliaciones políticas; afiliación sindical, gremial o asociativa; datos de salud; datos relativos a la vida sexual, afectiva u orientación sexual; datos biométricos; datos relativos al perfil biológico humano; y situación socioeconómica.

Regla General: Prohibición de Tratamiento. La Ley N° 21.719 establece como principio general que los datos sensibles no pueden ser tratados libremente. Su tratamiento sólo podrá realizarse cuando exista una autorización legal expresa o una base de licitud especialmente habilitada por la normativa. Esto implica que las organizaciones deben justificar de manera más rigurosa la necesidad de recopilar, utilizar, almacenar o comunicar este tipo de información.

Consentimiento Expreso y Reforzado. Como regla general, el tratamiento de datos sensibles requiere el consentimiento explícito del titular. Dicho consentimiento debe ser libre, previo, específico, informado, inequívoco y otorgado mediante una manifestación clara de voluntad. No resultan suficientes: casillas pre-marcadas, consentimientos implícitos, silencio del titular ni fórmulas ambiguas o genéricas.

Datos Biométricos: Protección Especial. Uno de los cambios más relevantes de la Ley N° 21.719 es la protección reforzada otorgada a los datos biométricos. Las organizaciones que utilicen control de acceso mediante huella digital, reconocimiento facial, sistemas biométricos de autenticación o plataformas de validación de identidad deberán evaluar cuidadosamente la base de licitud aplicable y las medidas de seguridad implementadas. Debido a que los datos biométricos son permanentes e irreemplazables, su tratamiento implica riesgos significativamente mayores que otros datos personales.

Obligaciones Especiales para las Organizaciones. Cuando una organización trate datos sensibles, debería implementar medidas reforzadas de cumplimiento: minimización, acceso restringido, medidas de seguridad reforzadas, conservación limitada, trazabilidad y evaluación de riesgos.

Recomendaciones para las PYMES. Antes de recopilar datos sensibles, toda organización debería preguntarse: ¿es realmente necesario tratar este dato?; ¿existe una base legal válida?; ¿se informó adecuadamente al titular?; ¿existen medidas de seguridad adecuadas?; y ¿la organización puede demostrar el cumplimiento?

¿Qué es el Tratamiento de Datos Personales?

El tratamiento de datos personales corresponde a cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por medios automatizados, tecnológicos, electrónicos, manuales o físicos. En términos simples, una organización realiza un tratamiento de datos personales cada vez que recopila, utiliza, almacena, organiza, consulta, modifica, comunica, comparte, conserva, bloquea, elimina o realiza cualquier otra acción respecto de información asociada a una persona natural identificada o identificable.

Por lo tanto, el tratamiento de datos personales no se limita al almacenamiento de información en una base de datos. La mayoría de las actividades que una empresa realiza con información de clientes, trabajadores, proveedores o usuarios constituyen tratamientos de datos personales.

Ejemplos habituales en una PYME

- Gestión de bases de datos de clientes y fichas de trabajadores.
- Reclutamiento y selección de personal.
- Videovigilancia y registro de visitas.
- Marketing y envío de comunicaciones comerciales.
- Formularios de contacto en sitios web, CRM, sistemas de facturación.
- Gestión de proveedores.
- Uso de plataformas en la nube y aplicaciones móviles.

Encargados de Tratamiento, Cesión de Datos y Transferencias Internacionales de Datos

Uno de los aspectos más relevantes de la Ley N° 21.719 consiste en distinguir claramente cuándo una organización está compartiendo datos con un proveedor que actúa por su cuenta, cuándo está cediendo datos a un tercero y cuándo está transfiriendo información fuera de Chile. Aunque estas figuras suelen confundirse en la práctica, tienen efectos jurídicos distintos y están sujetas a requisitos específicos.

1. Encargado de Tratamiento. Un Encargado de Tratamiento es una persona natural o jurídica que trata datos personales por cuenta de otra organización y siguiendo sus instrucciones (el "Responsable"). En este caso, el proveedor no utiliza los datos para fines propios, sino exclusivamente para prestar un servicio al Responsable del Tratamiento. El control de los datos sigue perteneciendo al Responsable.

Ejemplos: proveedor de almacenamiento en la nube, empresa de hosting, software de remuneraciones, servicio de correo masivo, plataforma CRM, call center, proveedor de soporte tecnológico y empresa de respaldo documental.

¿Cuándo se puede contratar un Encargado?

Cuando el tratamiento sea necesario para la prestación de un servicio legítimamente contratado por la organización y exista una base de licitud que permita el tratamiento original de los datos.

Requisitos

La organización debería:

- Identificar al proveedor.
- Evaluar sus medidas de seguridad.
- Formalizar un contrato o Acuerdo de Tratamiento o Procesamiento de Datos ("DPA") o establecer condiciones contractuales claras.
- Entregar instrucciones claras y documentadas.
- Supervisar razonablemente el cumplimiento del proveedor.

¿Qué debe regular el contrato?

Como mínimo:

- Objeto del tratamiento.
- Finalidades autorizadas.
- Medidas de seguridad.
- Confidencialidad.
- Subcontratación.
- Gestión de incidentes.
- Eliminación o devolución de datos al término del servicio.

¿Cuándo NO corresponde utilizar la figura de Encargado?

Cuando el tercero utiliza los datos para sus propios fines o toma decisiones independientes respecto de ellos. En esos casos ya no estamos frente a un Encargado, sino frente a una cesión de datos.

2. Cesión de Datos Personales. La cesión consiste en comunicar o transferir datos personales a un tercero para que éste los utilice para sus propios fines y bajo su propia responsabilidad. Una vez realizada la cesión, el tercero pasa a actuar como Responsable del Tratamiento respecto de los datos recibidos.

Ejemplos: entrega de bases de clientes a una empresa asociada, compartir información con una compañía de seguros, entregar datos a una institución financiera o compartir antecedentes con una empresa de marketing que utilizará los datos para sus propios fines.

¿Cuándo se puede realizar una cesión?

La cesión debe encontrarse respaldada por una base de licitud válida. Dependiendo del caso, podrá fundarse en:

- Consentimiento del titular.
- Cumplimiento de una obligación legal.
- Ejecución de un contrato.
- Otra hipótesis autorizada por la ley.

Deber de Información

La organización deberá informar a los titulares:

- Que sus datos serán cedidos a terceros.
- Quiénes serán dichos destinatarios.
- La finalidad de la cesión.
- La base de licitud que la justifica.

¿Cuándo NO se puede realizar una cesión?

No debería realizarse cuando:

- No existe una base de licitud válida.
- Se utilizan los datos para una finalidad incompatible con aquella para la cual fueron recopilados.
- El titular no ha sido informado cuando ello resulte exigible.
- La cesión vulnera los principios de finalidad, proporcionalidad o minimización.

.

3. Transferencias Internacionales de Datos. Existe una transferencia internacional cuando los datos personales son comunicados, almacenados, procesados o puestos a disposición fuera del territorio de Chile. Actualmente, muchas empresas realizan transferencias internacionales sin advertirlo.

Ejemplos: uso plataformas SaaS con servidores en el extranjero.

¿Cuándo se puede realizar una transferencia internacional?

La Ley N° 21.719 establece un régimen especial para las transferencias internacionales de datos personales. Como regla general, la transferencia será válida cuando exista un mecanismo legal que garantice un nivel adecuado de protección para los datos transferidos.

Entre los mecanismos contemplados por la normativa se encuentran:

- **País con nivel adecuado de protección:** Cuando el país receptor haya sido reconocido como adecuado por la autoridad competente.
- **Garantías contractuales adecuadas:** Mediante cláusulas contractuales, acuerdos o instrumentos jurídicos que otorguen protección equivalente a la exigida por la legislación chilena.
- **Consentimiento del titular:** En determinados casos previstos por la normativa.
- **Otras excepciones legales**: Cuando la transferencia sea necesaria para ejecutar un contrato, proteger derechos o cumplir obligaciones legalmente establecidas.

Obligaciones de las Empresas

Cuando existan transferencias internacionales, se recomienda:

- Identificar qué proveedores almacenan o procesan datos fuera de Chile.
- Informar esta circunstancia en la Política de Privacidad.
- Revisar las condiciones contractuales aplicables.
- Evaluar las medidas de seguridad del proveedor.
- Mantener evidencia de las garantías implementadas.
- Regular contractualmente la transferencia cuando corresponda.

Tabla Resumen

Figura	¿Quién decide el fin?	¿Usa datos propios?	¿Contrato?
Encargado de Tratamiento	El Responsable	No	Sí
Cesión de Datos	El tercero receptor	Sí	Recomendable
Transferencia Internacional	Depende del caso	Depende del rol que tenga el receptor	Sí, en la mayoría de los casos.

Recomendación para las PYMES

Uno de los errores más frecuentes consiste en asumir que cualquier proveedor tecnológico es un simple proveedor de servicios.

Antes de compartir datos personales con un tercero, la organización debería preguntarse:

1. ¿El tercero actúa siguiendo mis instrucciones o utiliza los datos para sus propios fines?
2. ¿Existe un contrato que regule el tratamiento?
3. ¿Los datos saldrán de Chile?
4. ¿He informado adecuadamente a los titulares?
5. ¿Existe una base de licitud que permita esta comunicación?

Responder correctamente estas preguntas permitirá determinar si se está frente a un Encargado de Tratamiento, una Cesión de Datos o una Transferencia Internacional, y aplicar las medidas de cumplimiento exigidas por la Ley N° 21.719.

¿Por qué es importante identificar los tratamientos?

La Ley N° 21.719 exige que las organizaciones conozcan y documenten los tratamientos de datos personales que realizan.

Esto permite:

- Identificar los datos tratados.
- Determinar la finalidad del tratamiento.
- Definir la base de licitud aplicable.
- Evaluar riesgos.
- Implementar medidas de seguridad.
- Atender solicitudes de los titulares.
- Demostrar cumplimiento ante una eventual fiscalización.

Si una organización realiza cualquier acción sobre información que permita identificar o hacer identificable a una persona natural, probablemente está realizando un tratamiento de datos personales y deberá cumplir con las obligaciones establecidas por la Ley N° 21.719.

Acciones mínimas recomendadas

- Elaborar un inventario de tratamientos de datos.
- Identificar qué datos se recopilan.
- Determinar la finalidad de cada tratamiento.
- Identificar responsables internos.
- Identificar sistemas y plataformas utilizadas.

Evidencia sugerida

- Inventario de tratamientos.
- Mapa de datos.
- Registro de sistemas que almacenan información personal.

1.2 Determinar la Base de Licitud de Cada Tratamiento

Todo tratamiento de datos personales debe sustentarse en una base legal válida establecida por la ley. La organización debe ser capaz de justificar por qué está autorizada para tratar cada conjunto de datos personales.

¿Qué es una base de licitud? La Ley N° 21.719 establece que ningún dato personal puede ser tratado libremente por una organización. Todo tratamiento debe encontrarse respaldado por una base de licitud o fundamento legal que autorice su realización. En términos simples, la base de licitud responde a la siguiente pregunta: **¿por qué la empresa está autorizada para recopilar, utilizar, almacenar, comunicar o eliminar estos datos personales?**

La identificación correcta de la base de licitud es uno de los elementos más importantes de un programa de cumplimiento, ya que determina las obligaciones aplicables, los derechos de los titulares y los riesgos asociados al tratamiento.

Una misma organización puede utilizar distintas bases de licitud dependiendo del tratamiento que realice.

Las principales bases de licitud aplicables para el caso de las pymes corresponden a las siguientes:

i. Consentimiento del Titular

El consentimiento es la manifestación de voluntad libre, específica, informada e inequívoca mediante la cual una persona autoriza el tratamiento de sus datos personales.

Para que sea válido, el titular debe conocer claramente:

- Quién tratará sus datos.
- Qué datos serán tratados.

- Para qué finalidad serán utilizados.
- Cómo puede revocar posteriormente su autorización.

El consentimiento no puede presumirse ni obtenerse mediante mecanismos ambiguos o poco transparentes.

Buenas prácticas

- Utilizar casillas no pre-marcadas.
- Mantener evidencia de la autorización otorgada.
- Permitir la revocación de manera simple.

ii. Ejecución de un Contrato

La empresa puede tratar datos personales cuando ello sea necesario para cumplir con una relación contractual con el titular.

No se requiere consentimiento cuando el tratamiento sea indispensable para cumplir el contrato.

Ejemplos

- Emisión de facturas.
- Entrega de productos.
- Prestación de servicios.
- Gestión de pagos.
- Atención postventa.
- Administración de contratos laborales.

Buenas prácticas

- Limitar el uso de los datos a lo necesario para el contrato.
- Evitar utilizar estos datos para finalidades distintas sin una base legal adicional.

iii. Cumplimiento de una Obligación Legal

El tratamiento es lícito cuando una ley obliga o autoriza expresamente a la organización a recopilar, conservar o comunicar determinados datos personales.

En estos casos el consentimiento no es necesario, ya que el fundamento proviene directamente de la ley.

Ejemplos

- Contratos de trabajo.
- Liquidaciones de sueldo.
- Cotizaciones previsionales.
- Registro de asistencia.
- Facturación.
- Conservación de antecedentes contables.
- Declaraciones tributarias.
- Prevención de lavado de activos.
- Cumplimiento normativo sectorial.
- Requerimientos de autoridades competentes.

Buenas prácticas

- Identificar claramente la norma legal que respalda el tratamiento.
- Mantener evidencia de dicha obligación.

iv. Interés Legítimo del Responsable

La ley permite tratar datos personales cuando exista un interés legítimo del responsable o de un tercero, siempre que dicho interés no prevalezca sobre los derechos y libertades fundamentales de los titulares.

Esta base requiere realizar un análisis previo que permita justificar el equilibrio entre el interés perseguido y los derechos de las personas.

Ejemplos

- Seguridad física de instalaciones.
- Videovigilancia.
- Prevención de fraude.
- Seguridad informática.
- Protección de activos de la empresa.
- Gestión de reclamos.
- Comunicaciones corporativas razonables con clientes existentes.

Buenas prácticas

- Realizar una evaluación de interés legítimo.
- Documentar el análisis efectuado.
- Aplicar medidas de mitigación cuando existan riesgos para los titulares.

Por ello, se recomienda elaborar una **Matriz de Tratamientos y Bases de Licitud**, que permita identificar claramente qué fundamento jurídico respalda cada actividad de tratamiento realizada por la organización.

Esta matriz será uno de los documentos más importantes para demostrar cumplimiento ante clientes, auditorías o eventuales fiscalizaciones de la Agencia de Protección de Datos Personales.

1.3 Informar Adecuadamente a los Titulares

La ley exige transparencia respecto del tratamiento de los datos personales. Las personas deben conocer quién trata sus datos, para qué fines, cuáles son sus derechos y cómo pueden ejercerlos.

Información mínima obligatoria:

- Identificación del responsable del tratamiento.
- Finalidades del tratamiento y base de licitud.
- Destinatarios y transferencias internacionales.
- Plazos de conservación.
- Derechos ARSOP-B del titular y canal de contacto.

Dónde informar

- Política de privacidad.
- Sitio web.
- Formularios de recolección.
- Contratos.
- Procesos de contratación laboral.
- Aplicaciones móviles.

Acciones mínimas recomendadas

- Elaborar una Política de Privacidad.
- Revisar formularios y contratos.
- Incorporar cláusulas informativas cuando corresponda.

1.4 Implementar Medidas de Seguridad

Las organizaciones deben proteger los datos personales mediante medidas técnicas y organizativas apropiadas al riesgo. La ley no exige una tecnología específica, sino medidas razonables y proporcionales según la realidad de cada empresa.

Ejemplos:

Organizacionales	Técnicas	Físicas
Política de protección de datos, responsables, capacitación, control de acceso.	Contraseñas robustas, MFA, antivirus, respaldos, cifrado cuando corresponda, Gestión de usuarios y perfiles.	Control de acceso a instalaciones, resguardo y destrucción segura de documentos.

1.5 Gestionar los Derechos de los Titulares (ARSOP-B)

La ley reconoce diversos derechos que pueden ser ejercidos por las personas respecto de sus datos personales.

¿Qué son los Derechos ARSOP?

La Ley N° 21.719 reconoce a todas las personas una serie de derechos destinados a garantizar el control sobre sus datos personales y permitirles intervenir activamente en la forma en que éstos son tratados por organizaciones públicas y privadas.

Estos derechos constituyen uno de los pilares fundamentales del nuevo sistema de protección de datos personales y obligan a las empresas a implementar mecanismos adecuados para recibir, gestionar y responder las solicitudes de los titulares.

Los principales derechos reconocidos por la ley son:

	Derecho	Descripción
A	Derecho de Acceso	Conocer si se tratan datos, categorías, finalidad, base de licitud, destinatarios, plazo de conservación y transferencias internacionales.
R	Derecho de Rectificación	Corregir o actualizar datos inexactos, incompletos, erróneos o desactualizados.
S	Derecho de Supresión	Eliminar datos cuando no sean necesarios para la finalidad declarada, se retire el consentimiento o el tratamiento sea ilícito.
O	Derecho de Oposición	Solicitar que la organización deje de tratar datos (ej.: publicidad, perfiles comerciales, tratamientos basados en interés legítimo).
P	Derecho de Portabilidad	Obtener una copia de los datos en formato estructurado e interoperable, o solicitar su transmisión a otro responsable.
B	Derecho de Bloqueo	Suspender temporalmente el tratamiento mientras se discute la exactitud de los datos o existe una reclamación pendiente.

i Toda organización debe disponer de un canal para recibir solicitudes ARSOP-B: correo electrónico, formulario web o canal de atención.

i. Derecho de Acceso

El derecho de acceso permite a una persona conocer si una organización está tratando sus datos personales y obtener información sobre dicho tratamiento.

En términos simples, permite al titular preguntar:

"¿Qué datos tienen sobre mí y qué están haciendo con ellos?"
El titular puede solicitar información sobre:

- Los datos personales que posee la empresa.
- El origen de los datos.
- Las finalidades del tratamiento.
- La base de licitud utilizada.
- Los destinatarios o terceros con quienes se comparten.
- El plazo de tratamiento
- Las transferencias internacionales realizadas.
- Las categorías de datos tratadas.
- Entre otros

Obligación de la empresa
La organización deberá proporcionar la información de manera clara, comprensible y gratuita, salvo excepciones legales expresamente establecidas.

ii**. Derecho de Rectificación**
Permite al titular solicitar la corrección o actualización de datos personales que sean inexactos, incompletos, erróneos o desactualizados.
Ejemplos

- Corrección de un nombre mal escrito.
- Actualización de domicilio.
- Cambio de correo electrónico.
- Corrección de antecedentes laborales.
- Actualización de información de contacto.

Obligación de la empresa
La organización deberá corregir los datos cuando la solicitud sea procedente y adoptar las medidas necesarias para mantener la consistencia de la información en sus sistemas.

iii. Derecho de Supresión
Permite solicitar la eliminación de datos personales cuando exista una causa legal que justifique dicha solicitud.
Procede cuando:

- Los datos ya no son necesarios para la finalidad que justificó su recopilación.
- El consentimiento ha sido revocado y no exista otra base legal.
- El tratamiento resulta ilícito.
- Ha expirado el plazo de conservación aplicable.
- Los datos fueron obtenidos o tratados de forma contraria a la ley.
- Entre otras

No procede cuando:
La organización deba conservar los datos para cumplir una obligación legal o contractual, entre otras excepciones.
Ejemplos

- Obligaciones tributarias.
- Registros laborales obligatorios.
- Conservación de antecedentes exigida por autoridades competentes.
- Defensa de derechos en procesos judiciales o administrativos.

iv. Derecho de Oposición

Permite al titular solicitar que la organización deje de tratar sus datos personales cuando existan circunstancias particulares que justifiquen dicha oposición.

Ejemplos

- Oposición al envío de publicidad.
- Oposición a perfiles comerciales.
- Oposición a determinadas actividades de marketing.
- Oposición a tratamientos basados en intereses legítimos.

.

Obligación de la empresa

La organización deberá evaluar la solicitud y cesar el tratamiento cuando no existan razones legítimas imperiosas que justifiquen su continuación.

v. Derecho de Portabilidad

Permite al titular obtener una copia de sus datos personales en un formato estructurado, de uso común e interoperable, y solicitar su transmisión a otro responsable cuando el tratamiento se realice de forma automatizada y esté basado en el consentimiento del titular.

Su finalidad es facilitar que las personas mantengan el control sobre su información y puedan cambiar de proveedor sin perder sus antecedentes.

Ejemplos

- Cambio de entidad financiera.
- Cambio de proveedor tecnológico.
- Migración entre plataformas digitales.
- Transferencia de información entre prestadores de servicios.

Obligación de la empresa

Entregar la información en un formato que permita su reutilización y lectura por otros sistemas.

vi. Derecho de Bloqueo

Permite al titular solicitar la suspensión temporal del tratamiento de sus datos personales en determinadas circunstancias.

Durante el período de bloqueo, los datos podrán conservarse, pero no podrán ser objeto de tratamiento activo, salvo para efectos de conservación o cumplimiento de obligaciones legales.

Procede, por ejemplo, cuando:

- Se impugna la exactitud de los datos.
- Se discute la procedencia de una solicitud de supresión.
- Existe una reclamación pendiente respecto del tratamiento.

Plazos para Responder Solicitudes de Derechos ARSOP

La Ley N° 21.719 exige que los responsables del tratamiento cuenten con procedimientos que permitan gestionar oportunamente las solicitudes de los titulares.

Como regla general, las solicitudes deberán ser respondidas dentro del plazo legal establecido por la normativa vigente y sus futuras instrucciones complementarias emitidas por la Agencia de Protección de Datos Personales.

El procedimiento debería contemplar:

- Recepción de la solicitud.
- Verificación de identidad del solicitante.
- Análisis de procedencia.
- Ejecución de las medidas correspondientes.
- Respuesta formal al titular.
- Registro y conservación de evidencia.

Toda PYME debería mantener un registro formal de las solicitudes recibidas.

Como mínimo, dicho registro debería contener:

- Fecha de recepción.
- Identificación del titular.
- Derecho ejercido.
- Responsable de la gestión.
- Análisis realizado.
- Fecha de respuesta.
- Resultado de la solicitud.
- Evidencia de la respuesta enviada.

Este registro constituye una de las principales evidencias de cumplimiento que podrá ser requerida durante auditorías o fiscalizaciones de la Agencia de Protección de Datos Personales.

Recomendación Práctica para las PYMES

Se recomienda elaborar un **Procedimiento de Gestión de Derechos de los Titulares (ARSOP)** y designar formalmente a uno o más responsables internos para su administración.

Acciones mínimas recomendadas

- Habilitar un canal de atención.
- Definir responsables internos.
- Crear un procedimiento de respuesta.
- Mantener registro de solicitudes recibidas.

La capacidad de responder oportunamente a las solicitudes de los titulares constituye uno de los principales indicadores de cumplimiento y madurez en materia de protección de datos personales. Incluso si la organización nunca ha recibido una solicitud, debe encontrarse preparada para gestionarla adecuadamente desde el primer día de vigencia de la Ley N° 21.719.

1.6 Regular la Relación con Proveedores (Encargados)

Muchas PYMES utilizan proveedores que acceden o procesan datos personales por su cuenta o por cuenta de la empresa.

Por ejemplo: servicios de nube, software de recursos humanos, plataformas de marketing, servicios tecnológicos, consultoras y call centers.

Cuando un proveedor trata datos por cuenta de la empresa, debe existir un acuerdo que regule dicho tratamiento.

Aspectos mínimos a regular

- Objeto y duración del encargo.
- Finalidad del tratamiento, tipo de datos personales tratados categorías de titulates
- Instrucciones del responsable.
- Obligaciones de las Partes.
- Confidencialidad.
- Medidas de seguridad.
- Subcontratación.
- Eliminación o devolución de datos.
- Gestión de incidentes.

Acciones mínimas recomendadas

- Identificar proveedores críticos.
- Revisar contratos vigentes.
- Incorporar anexos o acuerdos de tratamiento de datos cuando corresponda.

1.7 Gestionar Incidentes de Seguridad

Las organizaciones deben estar preparadas para detectar, contener, analizar y documentar incidentes que afecten la seguridad de los datos personales. Un incidente puede incluir: acceso no autorizado, pérdida de información, divulgación accidental, ataques informáticos, robo de dispositivos o envío erróneo de información, entre otros.

Acciones mínimas recomendadas

- Definir responsables.
- Establecer un procedimiento de respuesta.
- Crear canales internos de reporte.
- Mantener registros de incidentes.
- Evaluar la necesidad de notificaciones a la autoridad y titulares afectados.

⚠ Obligación de notificación a la Agencia de Protección de Datos dentro de 72 horas desde que el responsable toma conocimiento del incidente, cuando éste pueda causar daño significativo a los titulares.

1.8 Mantener Evidencia de Cumplimiento

La capacidad de demostrar cumplimiento es uno de los pilares centrales de la Ley N° 21.719. Ante una fiscalización, la empresa deberá acreditar las medidas implementadas y las decisiones adoptadas. No basta con declarar que se cumple; es necesario conservar evidencia objetiva.

- Inventario de tratamientos / Registro de Actividades de Tratamiento (RATs).
- Matriz de bases de licitud.
- Política de privacidad y política de protección de datos.
- Procedimiento ARSOP-B y procedimiento de gestión de incidentes.
- Contratos con proveedores (DPA cuando corresponda).
- Registros de capacitaciones, solicitudes de titulares e incidentes.
- Carpeta digital de cumplimiento consolidada.
- Entre otros.

Recomendación práctica para PYMES

Crear una carpeta digital de cumplimiento donde se almacenen todos los documentos, registros y evidencias relacionadas con la protección de datos personales.
Esta carpeta permitirá demostrar de manera simple, organizada y eficiente los esfuerzos de cumplimiento realizados por la organización.

Conclusión

La implementación de estas ocho obligaciones permitirá a la PYME construir una base sólida de cumplimiento frente a la Ley N° 21.719. La experiencia internacional demuestra que las organizaciones que comienzan tempranamente este proceso logran reducir riesgos legales, mejorar sus procesos internos y fortalecer la confianza de clientes, trabajadores y socios comerciales.

El siguiente capítulo presenta una metodología paso a paso para implementar estas obligaciones mediante un Plan de Adecuación diseñado específicamente para pequeñas y medianas empresas.

2. Metodología: 10 Pasos para el Plan de Adecuación

El cumplimiento de la Ley N° 21.719 no debe entenderse como un proceso exclusivamente jurídico ni como una carga administrativa imposible de abordar para una pequeña o mediana empresa. Por el contrario, puede implementarse de manera gradual, proporcional y práctica, priorizando aquellos tratamientos de datos que generen mayores riesgos para las personas y para la organización.

Este capítulo propone una metodología paso a paso para que una PYME pueda diseñar e implementar un Plan de Adecuación en Protección de Datos Personales, considerando sus recursos, tamaño, actividad económica y nivel de exposición al riesgo.

Paso	Etapa	Actividades Clave	Evidencia Sugerida
1	Designar Responsable Interno	Identificar a la persona o equipo encargado. Puede ser gerencia, administración, RRHH o tecnología. Definir funciones y crear carpeta de cumplimiento.	Acta o correo de designación. Lista de responsables. Carpeta de cumplimiento creada.
2	Levantar los Tratamientos (RATs)	Identificar todos los procesos donde se recopilan, usan, almacenan o eliminan datos personales. Revisar formularios, planillas, sistemas y plataformas. Identificar datos sensibles y terceros con acceso.	Inventario de tratamientos. Mapa de datos. Registro de Actividades de Tratamientos. Listado de sistemas y plataformas.
3	Determinar la Base de Licitud	Para cada tratamiento del inventario, asignar una base de licitud y documentar la justificación. Revisar consentimientos existentes. Elaborar análisis de interés legítimo cuando corresponda.	Matriz de bases de licitud. Formularios de consentimiento. Análisis de interés legítimo.
4	Diagnóstico y Análisis de Brechas	Comparar la situación actual con las exigencias legales. Clasificar hallazgos. Cada hallazgo podrá clasificarse como: **Cumple/Cumple Parcialmente/ No Cumple/ No Aplica. Priorizar por nivel de riesgo: Alto/ Medio/ Bajo.**	Informe de diagnóstico y brechas. Registro de hallazgos con acciones correctivas.
5	Implementar Acciones Correctivas	Para cada brecha detectada: definir acción correctiva, responsable, fecha de implementación y recursos.	Plan de adecuación con estado de avance. Registros de cierre de brechas.
6	Documentación de Cumplimiento	Elaborar: Política de Protección de Datos, Política de Privacidad, Política de Conservación y Eliminación, Política de Seguridad. Formalizar procedimientos ARSOP-B y gestión de incidentes.	Set documental completo. Contratos actualizados. DPA con proveedores críticos.
7	Implementar Procedimientos Internos	Operacionalizar las políticas: canal de recepción ARSOP-B, verificación de identidad, plazos de respuesta y registro. Procedimiento de incidentes, proveedores y conservación.	Procedimientos formalizados. Responsables definidos. Canales habilitados.
8	Implementar Medidas de Seguridad	Controles organizacionales: acceso, confidencialidad, segregación. Controles técnicos: contraseñas robustas, antivirus, respaldos, cifrado. Controles físicos: instalaciones, destrucción segura.	Registros de acceso. Evidencia de controles técnicos. Compromisos de confidencialidad firmados.

9	Capacitación y Sensibilización	Capacitar en: conceptos básicos, principios, bases de licitud, derechos ARSOP-B, confidencialidad, gestión de incidentes, medidas de seguridad y buenas prácticas.	Registro de asistencia. Material de capacitación. Evaluaciones de aprendizaje.
10	Seguimiento y Mejora Continua	Revisar periódicamente políticas, inventarios, contratos y proveedores. Analizar incidentes y solicitudes ARSOP-B. Evaluar nuevos riesgos. La adecuación es un proceso permanente.	Informes de revisión. Planes de acción. Actas de revisión.

Paso 1: Designar un Responsable Interno del Proyecto

La empresa debe identificar a una persona o equipo encargado de coordinar el proceso de adecuación.

No siempre será necesario contar con un área legal o de cumplimiento especializada. En una PYME, este rol puede ser asumido por la gerencia general, administración, recursos humanos, tecnología o quien tenga mayor conocimiento de los procesos internos.

Actividades recomendadas

- Designar formalmente a un responsable del proyecto.
- Definir sus funciones principales.
- Establecer apoyo de las áreas que tratan datos personales.
- Crear una carpeta digital de cumplimiento.

Evidencia sugerida

- Acta, correo o documento de designación.
- Lista de responsables por área.
- Carpeta de cumplimiento creada.

Paso 2: Levantar los Tratamientos de Datos Personales (Rats)

El segundo paso consiste en identificar todos los procesos de la empresa donde se recopilan, utilizan, almacenan, comunican o eliminan datos personales.

Este levantamiento permite conocer el punto de partida real de la organización.

Actividades recomendadas

- Revisar procesos de clientes, trabajadores, proveedores y usuarios.
- Identificar formularios, planillas, sistemas y plataformas.
- Identificar bases de datos y como fueron construidas
- Determinar qué datos se tratan y para qué finalidad.
- Identificar si existen datos sensibles.
- Identificar terceros que acceden a los datos.

Evidencia sugerida

- Inventario de tratamientos/Registro de Actividades de Tratamiento
- Mapa de datos.
- Listado de sistemas y plataformas.

Paso 3: Determinar la Base de Licitud

Cada tratamiento identificado debe contar con una base legal que lo justifique.

La empresa debe evitar asumir que todo se resuelve mediante consentimiento. En muchos casos, el tratamiento estará fundado en la ejecución de un contrato, el cumplimiento de una obligación legal o el interés legítimo.

Actividades recomendadas

- Revisar cada tratamiento del inventario.
- Asignar una base de licitud.
- Documentar la justificación.
- Revisar consentimientos existentes.
- Identificar tratamientos sin fundamento claro**.**

Evidencia sugerida

- Matriz de bases de licitud.
- Formularios de consentimiento.
- Análisis de interés legítimo, cuando corresponda.

Paso 4: Etapa de Diagnóstico y Análisis de Brechas

El diagnóstico constituye la base sobre la cual se construirá todo el programa de cumplimiento, ya que permite identificar las brechas existentes entre la situación actual de la empresa y las exigencias establecidas por la normativa.

Esta etapa debe ser proporcional al tamaño, complejidad y nivel de riesgo de la organización, privilegiando un enfoque práctico que permita obtener una visión clara de las actividades de tratamiento realizadas.

Identificación de Brechas

Con base en la evaluación realizada, deberán identificarse todas aquellas materias que requieran implementación, actualización o mejora.

Cada hallazgo podrá clasificarse como:

Cumple	Cumple Parcialmente	No Cumple	No Aplica
La organización dispone de controles adecuados y evidencia suficiente.	Existen medidas implementadas, pero requieren ajustes o formalización.	No existen medidas suficientes para cumplir con la obligación evaluada.	La obligación no resulta aplicable a la realidad de la organización.

Clasificación de Riesgos

Las brechas detectadas deberán priorizarse considerando su impacto potencial sobre los derechos de los titulares y sobre la organización.

Riesgo Alto	Riesgo Medio	Riesgo Bajo
Brechas que pueden generar incumplimientos significativos, afectar derechos fundamentales o exponer a la organización a sanciones relevantes.	Brechas que requieren corrección en el corto plazo para fortalecer el cumplimiento.	Aspectos de mejora o formalización documental que no generan una exposición inmediata.

Informe de Diagnóstico y Brechas

Como resultado de esta etapa, la organización deberá elaborar un Informe de Diagnóstico y Brechas que consolide los principales hallazgos identificados, incluyendo recomendaciones.

Modelo Simplificado de Registro de Hallazgos

N°	Hallazgo	Riesgo	Acción Correctiva	Responsable	Estado
1	No existe Política de Privacidad	Alto	Elaborar y publicar política	Gerencia	Cerrado
2	Contratos con proveedores sin cláusulas de datos	Alto	Incorporar anexos de tratamiento	Legal	En Proceso
3	No existe procedimiento ARSOP	Medio	Elaborar procedimiento	RRHH	Cerrado
4	Falta capacitación a trabajadores	Medio	Ejecutar capacitación anual	RRHH	Pendiente

Al finalizar esta etapa, la organización contará con una visión clara de su situación actual respecto de la protección de datos personales, identificará las brechas existentes y dispondrá de una hoja de ruta concreta para avanzar en su proceso de adecuación a la Ley N° 21.719.

El Informe de Diagnóstico y Brechas constituirá el principal insumo para la siguiente etapa: la implementación de las medidas correctivas y de cumplimiento necesarias para cerrar las brechas identificadas y fortalecer el programa de protección de datos personales de la organización.

Paso 5: Implementar Acciones Correctivas y Cierre de Brechas

Una vez finalizado el diagnóstico y levantamiento de información, la organización deberá analizar los hallazgos detectados y ejecutar las medidas necesarias para corregir las brechas de cumplimiento identificadas.

La finalidad de esta etapa es asegurar que los riesgos detectados durante el proceso de adecuación sean efectivamente mitigados mediante acciones concretas, responsables definidos y plazos de ejecución razonables.

La sola identificación de una brecha no constituye incumplimiento; el problema se intensifica cuando la organización conoce la existencia de una deficiencia y no adopta medidas para corregirla.

Actividades recomendadas

Identificación de Brechas

Analizar los resultados obtenidos durante el proceso de levantamiento y diagnóstico para identificar:

- Tratamientos sin base de licitud definida.
- Ausencia de políticas o procedimientos.
- Falta de información a titulares.
- Contratos sin cláusulas de protección de datos adecuadas.
- Proveedores sin regulación adecuada.
- Ausencia de medidas de seguridad.
- Deficiencias en la gestión de derechos ARSOP
- Falta de registros o evidencia documental.

Implementación de Medidas Correctivas

Para cada brecha detectada se recomienda definir:

- Acción correctiva.
- Responsable.
- Fecha de implementación.
- Recursos necesarios.
- Estado de avance.

Paso 6. Implementación y Actualización de la Documentación de Protección de Datos Personales

Una vez identificadas las brechas de cumplimiento, la organización deberá desarrollar, actualizar o formalizar la documentación necesaria para dar cumplimiento a las obligaciones establecidas por la Ley N° 21.719.

La documentación constituye uno de los principales mecanismos para demostrar cumplimiento, establecer responsabilidades internas y regular adecuadamente las relaciones con titulares, trabajadores, clientes, proveedores y terceros.

La complejidad y extensión de esta documentación deberá ser proporcional al tamaño, actividad y nivel de riesgo de la organización.

i. Políticas y Documentos Internos

La organización deberá elaborar o actualizar los documentos internos que regulen el tratamiento de datos personales y establezcan los criterios de actuación para trabajadores, colaboradores y terceros.

Entre los documentos relevantes a ser gestionados, se destacan los siguientes:

Política de Protección de Datos Personales

Documento que establece los principios, responsabilidades y reglas generales que deberá observar la organización respecto del tratamiento de datos personales.

Debería contemplar, al menos:

- Principios de tratamiento.
- Roles y responsabilidades.
- Bases de licitud.
- Medidas de seguridad.
- Gestión de incidentes.
- Derechos de los titulares.
- Conservación y eliminación de datos.
- Supervisión y mejora continua.

Política de Privacidad

Documento dirigido a los titulares de datos que informa de manera transparente cómo la organización recopila, utiliza, almacena, comunica y protege los datos personales.

Debería incluir:

- Identificación del responsable.
- Finalidades del tratamiento.
- Bases de licitud.
- Destinatarios de los datos.
- Transferencias internacionales.
- Plazos de conservación.
- Derechos de los titulares.
- Canales de contacto.

Política de Conservación y Eliminación de Datos

Documento que establece los criterios y plazos para conservar, anonimizar, bloquear o eliminar información personal.

Política de Seguridad de la Información

Documento que define las medidas organizacionales, físicas y técnicas destinadas a proteger los datos personales frente a accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas.

ii. Procedimientos

Los procedimientos permiten operacionalizar las obligaciones establecidas en las políticas internas.

Entre los documentos relevantes a ser gestionados, se destacan los siguientes:

- **Procedimiento de Gestión de Derechos ARSOP-B:** Regula la recepción, análisis y respuesta de solicitudes de acceso, rectificación, supresión, oposición, portabilidad y bloqueo**.**

- **Procedimiento de Gestión de Incidentes:** Establece las acciones necesarias para detectar, reportar, contener, analizar y documentar incidentes de seguridad que afecten datos personales.
- **Procedimiento de Gestión de Proveedores:** Define los controles que deben aplicarse antes de contratar proveedores que tengan acceso a datos personales.
- **Procedimiento de Conservación y Eliminación:** Regula la aplicación práctica de los plazos de conservación y destrucción de información.

Adecuación Contractual

La organización deberá revisar y actualizar sus contratos para incorporar las obligaciones derivadas de la Ley N° 21.719.

Entre los documentos relevantes a ser gestionados, se destacan los siguientes:

i. Contratos con Trabajadores

Se recomienda revisar:

- Contratos de trabajo/RIOHS.
- Anexos de contrato.
- Acuerdos de confidencialidad.
- Políticas internas incorporadas al Reglamento Interno cuando corresponda.

Las cláusulas deberían regular, entre otras materias:

- Confidencialidad.
- Acceso a información.
- Uso adecuado de sistemas.
- Protección de datos personales.
- Obligaciones posteriores al término de la relación laboral.

ii. Contratos con Clientes

Se recomienda incorporar cláusulas relativas a:

- Tratamiento de datos personales.
- Responsabilidades y obligaciones de las partes.
- Bases de licitud aplicables.
- Ejercicio de derechos de los titulares.
- Uso de plataformas tecnológicas.

iii. Contratos con Proveedores

Los contratos deberían contemplar obligaciones relacionadas con:

- Tratamiento de datos personales.
- Responsabilidades y obligaciones de las partes.

- Bases de licitud aplicables.
- Ejercicio de derechos de los titulares.
- Confidencialidad.
- Seguridad de la información.
- Gestión de incidentes.
- Subcontratación.
- Eliminación o devolución de información.
- Cumplimiento normativo.

iv. Acuerdos de Tratamiento de Datos (DPA)

Cuando un proveedor trate datos personales por cuenta de la organización, se recomienda formalizar un Acuerdo de Tratamiento de Datos Personales (Data Processing Agreement o DPA).

Este documento debería regular, al menos:

- Objeto del tratamiento.
- Categorías de datos.
- Finalidades autorizadas.
- Instrucciones del responsable.
- Medidas de seguridad.
- Subencargados.
- Transferencias internacionales.
- Gestión de incidentes.
- Auditorías.
- Devolución o eliminación de datos al término del servicio.

iii. Registros y Evidencia Documental

Además de las políticas, procedimientos y contratos, la organización deberá mantener evidencia documental que permita demostrar cumplimiento.

Registros mínimos recomendados

- Inventario de tratamientos.
- Registro de solicitudes ARSOP-B.
- Registro de incidentes.
- Registro de capacitaciones.
- Registro de proveedores.
- Matriz de bases de licitud.

- Matriz de riesgos.
- Plan de adecuación y seguimiento.

Resultado Esperado

Al finalizar esta etapa, la organización debería contar con un marco documental formalizado, actualizado y alineado con las exigencias de la Ley N° 21.719, compuesto por políticas, procedimientos, contratos, cláusulas y registros que permitan demostrar el cumplimiento de las obligaciones legales y sustentar el programa de protección de datos personales ante clientes, titulares, auditores y la Agencia de Protección de Datos Personales.

Paso 7: Implementación de Procedimientos Internos

Una vez definida la documentación, la organización deberá implementar procedimientos que permitan gestionar de forma consistente las obligaciones establecidas por la ley.

Estos procedimientos transforman las obligaciones legales en actividades operativas concretas.

Entre los documentos relevantes a ser gestionados, se destacan los siguientes:

i. Procedimiento de Gestión de Derechos ARSOP

Debe regular la forma en que la organización recibe, analiza y responde solicitudes de acceso, rectificación, supresión, oposición, portabilidad y bloqueo.

El procedimiento debería contemplar:

- Canal de recepción.
- Verificación de identidad.
- Responsable de gestión.
- Plazos de respuesta.
- Registro de solicitudes.
- Conservación de evidencia.

ii. Procedimiento de Transparencia e Información

Debe regular la forma en que la organización informa a los titulares sobre el tratamiento de sus datos personales.

El procedimiento debería considerar:

- Elaboración y actualización de políticas de privacidad.
- Revisión de formularios y contratos.
- Publicación de avisos de privacidad.
- Mecanismos para informar cambios relevantes.
- Controles de actualización periódica.

iii. Procedimiento de Gestión de Incidentes

Debe establecer las acciones necesarias para detectar, reportar, contener, analizar y documentar incidentes de seguridad que afecten datos personales.

iv. Procedimiento de Gestión de Proveedores

Debe regular la contratación, evaluación y supervisión de proveedores que accedan o traten datos personales.

v. Procedimiento de Conservación y Eliminación de Datos

Debe definir los plazos de conservación y los mecanismos de eliminación, anonimización o bloqueo de información.

Resultado esperado

La organización cuenta con procedimientos formalizados y responsables claramente definidos para gestionar sus principales obligaciones legales.

Paso 8. Implementación de Medidas de Seguridad

La Ley N° 21.719 exige adoptar medidas de seguridad apropiadas al riesgo del tratamiento realizado.

Las medidas deberán ser razonables, proporcionales y adecuadas a la naturaleza de los datos tratados.

Ejemplo:

Organizacionales	Técnicas	Físicas
Definición de responsables, Control de acceso a la información, Gestión de permisos, Compromisos de confidencialidad. Segregación de funciones cuando corresponda.	Contraseñas robustas, antivirus, respaldos, cifrado cuando corresponda, Gestión de usuarios y perfiles.	Control de acceso a instalaciones., Resguardo de archivos físicos, Destrucción segura de documentos, Protección de equipos dispositivos.

Resultado esperado

La organización cuenta con medidas de seguridad acordes a los riesgos identificados y puede demostrar su implementación mediante registros y evidencias.

Paso 9. Capacitación y Sensibilización

La protección de datos personales requiere que trabajadores, ejecutivos y colaboradores conozcan sus obligaciones y comprendan los riesgos asociados al tratamiento de datos personales.

La capacitación constituye una medida fundamental para prevenir errores humanos e incidentes de seguridad.

Contenidos mínimos recomendados

- Conceptos básicos de protección de datos personales.
- Principios de la Ley N° 21.719.
- Bases de licitud.
- Derechos ARSOP-B.
- Obligaciones de confidencialidad.
- Gestión de incidentes.
- Medidas de seguridad.

- Buenas prácticas en el tratamiento de datos.

Evidencias recomendadas

- Registro de asistencia.
- Material de capacitación.
- Presentaciones utilizadas.
- Comunicaciones internas.
- Evaluaciones o controles de aprendizaje.

Resultado esperado

Los trabajadores conocen sus responsabilidades y cuentan con herramientas para actuar adecuadamente frente a situaciones relacionadas con el tratamiento de datos personales.

Paso 10. Seguimiento y Mejora Continua

La adecuación a la Ley N° 21.719 no constituye un proyecto puntual, sino un proceso permanente de revisión y mejora.

La organización deberá monitorear periódicamente la efectividad de las medidas implementadas y realizar los ajustes necesarios cuando cambien los riesgos, procesos o requisitos legales.

Actividades recomendadas

- Revisar periódicamente políticas y procedimientos.
- Actualizar inventarios de tratamientos.
- Revisar contratos y proveedores.
- Analizar incidentes ocurridos y lecciones aprendidas.
- Revisar solicitudes ARSOP-B recibidas.
- Evaluar nuevos riesgos derivados de cambios tecnológicos u organizacionales.
- Actualizar programas de capacitación.

Evidencias recomendadas

- Informes de revisión periódica.
- Actualizaciones documentales.
- Planes de acción.
- Registros de seguimiento.
- Actas de revisión.

Resultado esperado

La organización mantiene un programa de protección de datos personales actualizado, efectivo y alineado con la evolución de sus actividades y de la normativa aplicable, pudiendo demostrar en todo momento el cumplimiento del principio de responsabilidad demostrable exigido por la Ley N° 21.719.

3. Carta Gantt de Adecuación – Junio a Noviembre 2026

Objetivo: Alcanzar un nivel adecuado de cumplimiento antes de la entrada en vigencia de la Ley N° 21.719 el 1 de diciembre de 2026.

Plazos orientativos efectos de dar cumplimiento a la norma antes de su entrada en vigencia:

Actividad	Jun	Jul	Ago	Sep	Oct	Nov
Designación de responsable interno	●					
Aplicación de cuestionario de autodiagnóstico	●					
Levantamiento de tratamientos (RATs)	●	●				
Elaboración inventario de tratamientos		●	●			
Identificación de bases de licitud			●			
Elaboración de informe de brechas			●			
Aprobación del plan de adecuación			●			
Política de Privacidad y de Protección de Datos			●	●		
Política de Seguridad y de Conservación				●		
Procedimiento ARSOP-B				●		
Procedimiento de Gestión de Incidentes				●	●	
Procedimiento de Gestión de Proveedores				●	●	
Revisión formularios y avisos de privacidad				●	●	
Revisión de contratos con clientes					●	
Revisión de contratos laborales / RIOHS					●	
Revisión de contratos con proveedores					●	●
Firma de DPA con proveedores críticos					●	●
Implementación de medidas de seguridad					●	●
Capacitación a trabajadores y jefaturas	●	●				

✓ Meta Final: Llegar al 1 de diciembre de 2026 con un programa de cumplimiento documentado, implementado y con evidencia suficiente para demostrar el principio de responsabilidad demostrable exigido por la Ley N° 21.719.

4. Cuestionario de Autodiagnóstico de Cumplimiento

El presente cuestionario tiene por finalidad permitir que la organización evalúe preliminarmente su nivel de preparación frente a las obligaciones establecidas por la Ley N° 21.719. Las respuestas permitirán identificar fortalezas, brechas de cumplimiento y prioridades de implementación.

I. Gobernanza y Gestión de Datos

Pregunta	Sí	Parcial	No	N/A
¿La organización ha designado a una persona responsable de coordinar materias de protección de datos?	☐	☐	☐	☐
¿Existen roles y responsabilidades definidas respecto del tratamiento de datos personales?	☐	☐	☐	☐
¿La alta dirección conoce las obligaciones de la Ley N° 21.719?	☐	☐	☐	☐
¿La organización ha iniciado formalmente un proceso de adecuación a la ley?	☐	☐	☐	☐

II. Inventario de Datos Personales

Pregunta	Sí	Parcial	No	N/A
¿La organización sabe qué datos personales recopila?	☐	☐	☐	☐
¿Se encuentran identificadas las finalidades para las cuales se utilizan los datos?	☐	☐	☐	☐
¿Se conoce dónde se almacenan los datos personales?	☐	☐	☐	☐
¿Se encuentran identificados los sistemas y plataformas que almacenan datos personales?	☐	☐	☐	☐
¿Se han identificado los datos sensibles tratados por la organización?	☐	☐	☐	☐
¿Existe un inventario o Registro de Actividades de Tratamiento (RATs)?	☐	☐	☐	☐

III. Bases de Licitud

Pregunta	Sí	Parcial	No	N/A
¿La organización ha identificado la base legal que justifica cada tratamiento de datos personales?	☐	☐	☐	☐
¿Se mantiene evidencia de los consentimientos obtenidos cuando corresponde?	☐	☐	☐	☐
¿Se revisan periódicamente los consentimientos otorgados por los titulares?	☐	☐	☐	☐
¿Se encuentran documentadas las situaciones en que se utiliza interés legítimo como base de licitud?	☐	☐	☐	☐

IV. Transparencia y Deber de Información

Pregunta	Sí	Parcial	No	N/A
¿La organización cuenta con una Política de Privacidad vigente?	☐	☐	☐	☐
¿La Política de Privacidad se encuentra disponible para los titulares?	☐	☐	☐	☐
¿Los formularios de recopilación contienen información adecuada sobre el tratamiento?	☐	☐	☐	☐
¿Los contratos incorporan cláusulas informativas cuando corresponde?	☐	☐	☐	☐
¿Se informa a los titulares sobre sus derechos ARSOP-B?	☐	☐	☐	☐

V. Derechos de los Titulares (ARSOP-B)

Pregunta	Sí	Parcial	No	N/A
¿Existe un canal para que los titulares ejerzan sus derechos?	☐	☐	☐	☐
¿Existe un procedimiento documentado para gestionar solicitudes ARSOP-B?	☐	☐	☐	☐
¿Se encuentra definido quién responde estas solicitudes?	☐	☐	☐	☐
¿Existe un registro de solicitudes recibidas y respuestas otorgadas?	☐	☐	☐	☐
¿La organización conoce los plazos legales para responder solicitudes?	☐	☐	☐	☐

VI. Seguridad de la Información

Pregunta	Sí	Parcial	No	N/A
¿Existen controles de acceso a los sistemas que contienen datos personales?	☐	☐	☐	☐
¿Se utilizan contraseñas robustas?	☐	☐	☐	☐
¿Se utiliza autenticación multifactor o similar en sistemas críticos?	☐	☐	☐	☐
¿Se realizan respaldos periódicos de la información?	☐	☐	☐	☐
¿Existe una política o procedimiento de seguridad de la información?	☐	☐	☐	☐
¿Los trabajadores han suscrito compromisos de confidencialidad?	☐	☐	☐	☐
¿Existen procedimientos para eliminar información de forma segura?	☐	☐	☐	☐

VII. Gestión de Incidentes

Pregunta	Sí	Parcial	No	N/A
¿Existe un procedimiento para gestionar incidentes de seguridad?	☐	☐	☐	☐
¿Los trabajadores saben cómo reportar un incidente?	☐	☐	☐	☐
¿Existe un responsable para coordinar la gestión de incidentes?	☐	☐	☐	☐
¿Se mantiene un registro de incidentes ocurridos?	☐	☐	☐	☐
¿La organización conoce su obligación de notificar a la Agencia cuando corresponda?	☐	☐	☐	☐

VIII. Proveedores y Encargados de Tratamiento

Pregunta	Sí	Parcial	No	N/A
¿La organización ha identificado qué proveedores acceden a datos personales?	☐	☐	☐	☐
¿Existe un registro de dichos proveedores?	☐	☐	☐	☐
¿Los contratos regulan adecuadamente la protección de datos personales?	☐	☐	☐	☐
¿Existen Acuerdos de Tratamiento de Datos (DPA) cuando corresponde?	☐	☐	☐	☐
¿Los proveedores son evaluados desde una perspectiva de seguridad y privacidad?	☐	☐	☐	☐

IX. Capacitación y Cultura Organizacional

Pregunta	Sí	Parcial	No	N/A
¿Los trabajadores han recibido capacitación sobre protección de datos personales?	☐	☐	☐	☐
¿Los trabajadores conocen sus obligaciones de confidencialidad?	☐	☐	☐	☐
¿Existe material o comunicación interna sobre protección de datos?	☐	☐	☐	☐
¿La capacitación se realiza de manera periódica?	☐	☐	☐	☐

X. Evidencia y Cumplimiento

Pregunta	Sí	Parcial	No	N/A

¿La organización mantiene evidencia de cumplimiento de sus obligaciones?	☐	☐	☐	☐
¿Se conservan registros de capacitaciones, solicitudes e incidentes?	☐	☐	☐	☐
¿Existe una carpeta o repositorio de cumplimiento?	☐	☐	☐	☐
¿Se revisan periódicamente las políticas y procedimientos?	☐	☐	☐	☐
¿La organización cuenta con un plan de mejora continua en materia de protección de datos?	☐	☐	☐	☐

5. Preguntas Frecuentes (FAQ)

Adecuación a la Ley N° 21.719 sobre Protección de Datos Personales

1. ¿Mi empresa está obligada a cumplir la Ley N° 21.719?
Sí. La ley aplica a toda organización pública o privada que trate datos personales de personas naturales, independientemente de su tamaño. Si su empresa mantiene información de clientes, trabajadores, proveedores, postulantes a empleo, contactos comerciales o usuarios de un sitio web, se encuentra sujeta a esta normativa.

2. ¿Qué son los datos personales y qué es el tratamiento?
Datos personales: Son todos aquellos datos que permiten identificar o hacer identificable a una persona natural. Ejemplos: nombre, RUT, dirección, correo electrónico, teléfono, patente de vehículo asociada a una persona, dirección IP, datos laborales e imágenes de una persona. Tratamiento de datos personales: corresponde a cualquier operación o actividad realizada sobre datos personales, ya sea por medios manuales, electrónicos o automatizados. Se considera tratamiento, entre otras actividades: recopilar datos, registrar información, organizar bases de datos, almacenar información, consultar registros, utilizar datos para prestar servicios, compartir información con proveedores, enviar correos electrónicos, actualizar antecedentes, conservar documentos y eliminar o destruir información.

3. ¿Qué son los datos sensibles?
Son datos que requieren una protección reforzada debido a que pueden afectar significativamente la privacidad o derechos de las personas. Ejemplos: datos de salud, datos biométricos, origen racial o étnico, convicciones religiosas o filosóficas, información sobre la vida sexual y afiliación sindical.

4. ¿Necesito pedir consentimiento para todos los tratamientos de datos?
No. El consentimiento es solo una de las bases de licitud previstas por la ley (con excepción de los datos sensibles). En muchos casos el tratamiento puede fundarse en: ejecución de un contrato, cumplimiento de una obligación legal, interés legítimo, protección de intereses vitales u otras bases reconocidas por la ley.

5. ¿Qué es una base de licitud?
Es el fundamento legal que autoriza a la organización a tratar datos personales. Antes de recopilar o utilizar datos personales, la empresa debe ser capaz de responder: ¿por qué estoy autorizado a tratar estos datos?

6. ¿Qué es un inventario de tratamientos?
Es un registro que identifica los tratamientos de datos personales realizados por la organización. Debe indicar, entre otros aspectos: qué datos se tratan, para qué finalidad, dónde se almacenan, quién accede a ellos y cuál es la base de licitud aplicable.

7. ¿Mi empresa necesita una Política de Privacidad?
Sí. Toda organización que recopile datos personales debería contar con una Política de Privacidad que informe de manera transparente qué datos recopila, para qué los utiliza, cuál es la base de licitud, con quién los comparte y qué derechos tienen los titulares, entre otros.

8. ¿Qué son los derechos ARSOP-B?
Son los derechos que la ley reconoce a los titulares respecto de sus datos personales. Incluyen: Acceso, Rectificación, Supresión, Oposición, Portabilidad y Bloqueo. La empresa debe estar preparada para responder solicitudes relacionadas con estos derechos.

9. ¿Debo habilitar un canal para recibir solicitudes ARSOP-B?
Sí. La organización debe disponer de un mecanismo que permita a los titulares ejercer sus derechos. Puede tratarse de un correo electrónico, un formulario web, una plataforma de atención o un canal de servicio al cliente.

10. ¿Qué ocurre si un titular solicita eliminar sus datos?
La empresa deberá analizar si la solicitud procede. Si no existe una obligación legal o contractual o base de licitud que justifique la conservación de los datos, deberá eliminarlos o anonimizar la información cuando corresponda.

11. ¿Necesito un procedimiento para gestionar incidentes de seguridad?
Sí. Toda organización debería contar con un procedimiento que permita detectar incidentes, reportarlos internamente, evaluar su impacto, implementar medidas de contención y documentar lo ocurrido.

12. ¿Qué se considera un incidente de seguridad?
Cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de datos personales. Ejemplos: robo de computadores, acceso no autorizado, pérdida de información, ataques informáticos, envío erróneo de correos y exposición accidental de bases de datos.

13. ¿Qué pasa si utilizo servicios en la nube?
La utilización de servicios cloud no está prohibida. Sin embargo, la empresa sigue siendo responsable de verificar que el proveedor implemente medidas adecuadas de seguridad y protección de datos.

14. ¿Qué es un Encargado de Tratamiento?
Es una persona o empresa que trata datos personales por cuenta de otra organización. Ejemplos: proveedores de software, plataformas SaaS, empresas de almacenamiento en la nube, servicios de recursos humanos y empresas de marketing.

15. ¿Necesito firmar contratos especiales con estos proveedores?
Sí, cuando traten datos personales por cuenta de la organización. Se recomienda suscribir un Acuerdo de Tratamiento de Datos Personales (DPA) o incorporar cláusulas específicas de protección de datos en el contrato correspondiente.

16. ¿Qué medidas de seguridad exige la ley?
La ley no establece una tecnología específica. Exige que las organizaciones implementen medidas apropiadas al riesgo. Ejemplos: contraseñas robustas, autenticación multifactor, respaldos, control de accesos, capacitación, confidencialidad y protección física de documentos.

17. ¿Necesito capacitar a mis trabajadores?
Sí. La capacitación constituye una de las medidas más eficaces para prevenir errores humanos, incidentes de seguridad y tratamientos indebidos de datos personales.

18. ¿Qué documentación mínima debería tener una PYME?
Como mínimo se recomienda contar con: Política de Privacidad, Política de Protección de Datos, Procedimiento ARSOP-B, Procedimiento de Gestión de Incidentes, Registro de Proveedores, cláusulas contractuales de protección de datos, Acuerdos de Tratamiento de Datos cuando corresponda y evidencia de capacitación.

19. ¿Qué significa el principio de responsabilidad demostrable?
Significa que no basta con cumplir la ley; la organización debe ser capaz de demostrar que cumple. Por ello, resulta fundamental mantener evidencia de: políticas, procedimientos, registros, capacitaciones, contratos y evaluaciones realizadas.

20. ¿Qué pasa si mi empresa aún no ha comenzado su proceso de adecuación?
Todavía existe tiempo para prepararse antes de la entrada en vigencia general de la Ley N° 21.719. Sin embargo, se recomienda iniciar el proceso lo antes posible, ya que la adecuación requiere revisar contratos, procesos, sistemas, proveedores y documentación interna. Las organizaciones que comiencen tempranamente podrán reducir riesgos y evitar costos asociados a adecuaciones de última hora.

21. ¿Cuál es el primer paso que debería dar mi empresa?
Realizar un autodiagnóstico. A partir de dicho diagnóstico será posible identificar los tratamientos de datos personales, detectar brechas de cumplimiento, priorizar riesgos, elaborar un plan de adecuación e implementar las medidas necesarias para cumplir con la Ley N° 21.719. El cuestionario de autodiagnóstico incluido en esta guía constituye un excelente punto de partida para comenzar ese proceso.

22. ¿Qué pasa si no cumplo con la Ley N° 21.719?

El incumplimiento de la Ley N° 21.719 puede dar lugar a fiscalizaciones y sanciones por parte de la Agencia de Protección de Datos Personales, incluyendo multas de hasta 5.000 UTM para infracciones leves, 10.000 UTM para infracciones graves y 20.000 UTM para infracciones gravísimas. Además, la Agencia podrá ordenar medidas correctivas y los titulares de los datos podrán ejercer acciones judiciales para proteger sus derechos y reclamar indemnizaciones. A ello se suman riesgos reputacionales, pérdida de confianza y potenciales impactos comerciales para la organización.

6. Exclusión de Responsabilidad y Consideraciones Interpretativas

⚠ La presente guía tiene fines exclusivamente informativos, educativos y referenciales.

⚠ No constituye asesoría legal, opinión jurídica ni garantía de cumplimiento normativo.

⚠ La utilización de estos documentos no reemplaza el análisis específico que cada organización debe realizar.

La presente guía, junto con los modelos, cláusulas, procedimientos, políticas, formularios y demás documentos, tiene fines exclusivamente informativos, educativos y referenciales. Su contenido ha sido elaborado con el propósito de apoyar a las pequeñas y medianas empresas en sus procesos de adecuación a la Ley N° 21.719 sobre Protección de Datos Personales. Sin embargo, no constituye asesoría legal, opinión jurídica, auditoría de cumplimiento, certificación, garantía de cumplimiento normativo ni reemplaza el análisis específico que cada organización debe realizar respecto de sus actividades de tratamiento de datos personales.

La utilización total o parcial de los documentos puestos a disposición no garantiza el cumplimiento de la normativa aplicable ni asegura la inexistencia de riesgos legales, regulatorios, contractuales, operacionales o reputacionales. Si bien se han realizado esfuerzos razonables para asegurar la calidad, actualidad y precisión de la información contenida en esta guía, no se garantiza que el contenido se encuentre libre de errores, omisiones, inexactitudes, interpretaciones alternativas o referencias que puedan quedar desactualizadas con posterioridad a su publicación.

La protección de datos personales constituye una materia jurídica, tecnológica y organizacional en constante evolución. Por ello, determinadas recomendaciones, ejemplos, interpretaciones o buenas prácticas incluidas en este documento podrían ser objeto de revisión, actualización o reinterpretación como consecuencia de cambios normativos, reglamentarios, tecnológicos, jurisprudenciales o de criterios emitidos por la Agencia de Protección de Datos Personales u otras autoridades competentes.

Los usuarios de esta guía aceptan que su utilización se realiza bajo su propia responsabilidad y reconocen que la adopción de decisiones de cumplimiento requiere considerar las circunstancias particulares de cada organización, sus actividades de tratamiento, riesgos específicos y obligaciones legales aplicables. En consecuencia, los autores, colaboradores, patrocinadores o entidades que participen en la elaboración o difusión de esta guía no garantizan la exactitud absoluta, integridad o vigencia permanente de su contenido, ni asumirán responsabilidad por errores involuntarios, omisiones, interpretaciones divergentes o decisiones adoptadas sobre la base de la información aquí contenida.

Cada organización es responsable de evaluar sus propias circunstancias, identificar los tratamientos de datos personales que realiza, determinar las bases de licitud aplicables, implementar medidas de seguridad adecuadas y adoptar las medidas de cumplimiento que resulten necesarias de acuerdo con su realidad particular. Se recomienda que, frente a situaciones específicas, tratamientos de alto riesgo, datos sensibles, transferencias internacionales, incidentes de seguridad, fiscalizaciones o dudas de interpretación normativa, la organización obtenga asesoría profesional especializada.

La Ley N° 21.719 incorpora diversas obligaciones, principios y conceptos jurídicos cuyo alcance práctico deberá ser precisado progresivamente mediante reglamentos, instrucciones generales, criterios interpretativos, resoluciones administrativas, pronunciamientos de la Agencia de Protección de Datos Personales y jurisprudencia de los tribunales de justicia.

En consecuencia, algunas materias abordadas en la presente guía pueden estar sujetas a distintas interpretaciones razonables y podrían evolucionar o modificarse en el futuro como resultado del desarrollo regulatorio y jurisprudencial de la normativa. Los criterios, recomendaciones, ejemplos y buenas prácticas contenidos en este documento reflejan una interpretación técnica efectuada a la fecha de su elaboración y tienen por objeto facilitar la comprensión e implementación práctica de la Ley N° 21.719 por parte de pequeñas y medianas empresas. Sin embargo, no constituyen interpretaciones oficiales ni vinculantes para

la Agencia de Protección de Datos Personales, los tribunales de justicia o cualquier otra autoridad competente.

En consecuencia, se recomienda revisar periódicamente la normativa vigente y mantener actualizados los programas de cumplimiento, políticas y procedimientos de protección de datos personales conforme evolucionen los criterios regulatorios y las buenas prácticas del sector. Frente a situaciones específicas, tratamientos de alto riesgo, datos sensibles, transferencias internacionales, incidentes de seguridad, fiscalizaciones o dudas de interpretación normativa, se recomienda obtener asesoría profesional especializada.