

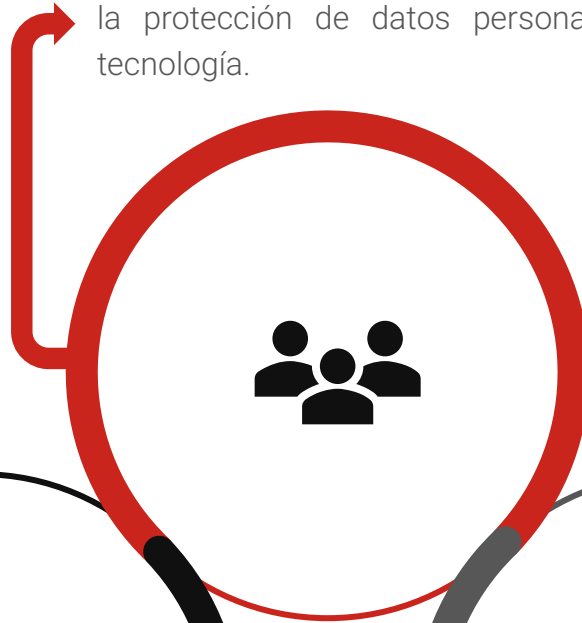
USO PÚBLICO | OCTUBRE 2025

Guía esencial en Protección de Datos Personales en Chile y Colombia

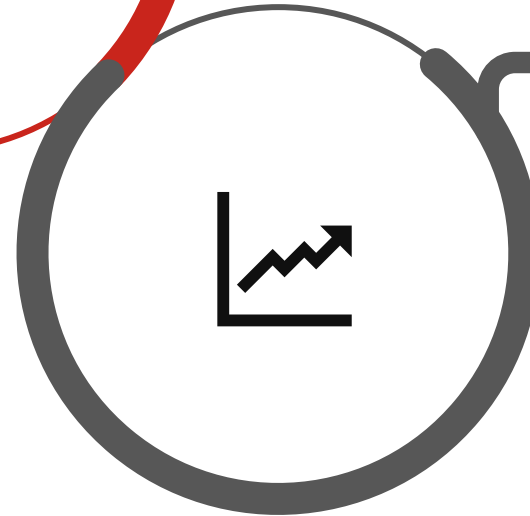
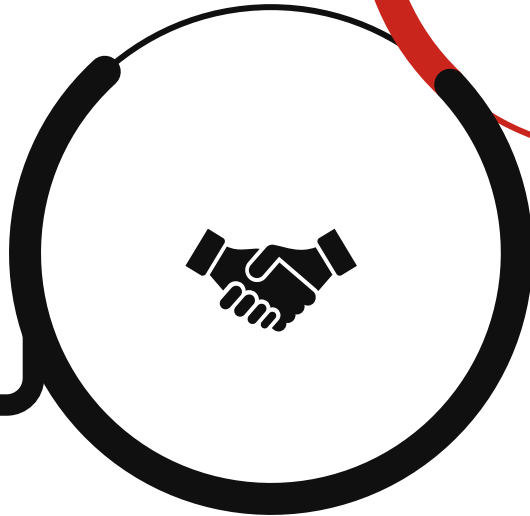
ECIJA

SOBRE EL EQUIPO ECIJA

En ECIJA contamos con un equipo multidisciplinario dedicado exclusivamente a la protección de datos personales y áreas de práctica especializadas en tecnología.



La estrecha colaboración entre nuestras oficinas nos permite ofrecer soluciones integrales y consistentes a organizaciones locales y multinacionales que operan en ambos mercados.



Nuestra trayectoria incluye la implementación de programas de cumplimiento, la defensa en procedimientos sancionatorios ante la Autoridad de Protección de Datos y la adaptación de modelos corporativos a los estándares de cada país.

CHILE Y COLOMBIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

01. ¿Qué regula la normativa?

Chile: La Ley N°19.628 modificada por la Ley N°21.719, regula la forma y condiciones en la cual se efectúa el tratamiento y protección de datos personales de conformidad al artículo 19 N° 4 de la Constitución Política de la República.

Colombia: La Ley 1581 de 2012 regula el tratamiento de los datos personales de las personas recogidos en bases de datos o archivos (públicos y privados), así como los derechos, libertades y garantías constitucionales que se refieren en el artículo N° 15 y N° 20 de la Constitución Política.

02. ¿Cuáles son los derechos de los titulares?

Chile: Los titulares tienen derecho a los denominados derechos **BARSOP**: Bloqueo, Acceso, Rectificación, Supresión, Oposición y Portabilidad. El responsable de datos debe implementar mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos de forma expedita, ágil y eficaz.

Colombia: Los titulares tienen derecho a conocer y rectificar los datos, para acceder a la información, solicitar prueba de la autorización otorgada, presentar quejas ante la Superintendencia de Industria y Comercio ("SIC") y a revocar la autorización y/o solicitar la supresión del dato.

03. ¿Qué deberes tiene la empresa?

Chile: El responsable deberá adecuar su tratamiento a los estándares establecidos en la normativa. Junto a ello, se reconoce el deber de secreto, información y transparencia, protección desde el diseño y por defecto, de adoptar medidas de seguridad apropiadas y de reportar las vulneraciones.

Colombia: El responsable deberá garantizar a los titulares el ejercicio de sus derechos y también informarles íntegramente respecto de sus solicitudes, conservar sus datos de manera segura y suministrar correctamente su información a los encargados. Asimismo, deberá adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley e informar a la autoridad cuando se presenten violaciones a los códigos de seguridad.

04. ¿Cómo se deben tratar los datos sensibles?

Chile: Sólo puede realizarse con el consentimiento expreso, otorgado por el titular de forma escrita, verbal o por medios tecnológicos. Existen otras excepciones como que sean datos públicos, sea una entidad sin fines de lucro, para salvaguardar la vida, formular una defensa jurídica, en cumplimiento de una obligación legal o cuando ésta así lo mandate.

Colombia: El tratamiento de datos personales sensibles requiere una autorización calificada del titular. Este deberá ser informado de manera expresa sobre las finalidades específicas del tratamiento y sobre cuáles de sus datos son sensibles. En ningún caso podrá condicionarse la prestación de un servicio al suministro de datos sensibles, como los biométricos.

CHILE Y COLOMBIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

05. Encargados de tratamiento de datos personales

Chile: El tratamiento se puede realizar por un tercero mandatario conforme a las instrucciones que se le impartan. Para ello, se debe celebrar un contrato en el que se establecerá el objeto del encargo, su duración, finalidad, el tipo de datos tratados, las categorías de los titulares y los derechos y obligaciones de las partes.

Colombia: Además de los deberes previstos en la ley, el encargado deberá cumplir las instrucciones del responsable conforme al contrato de transmisión de datos, aplicar las obligaciones derivadas de la política de tratamiento del responsable y garantizar que éste se realice únicamente para las finalidades autorizadas por los titulares y en cumplimiento de la normativa aplicable.

07. Notificación de incidentes de seguridad

Chile: Se debe reportar a la Agencia de Protección de Datos Personales ("AGPD") por los medios más expeditos posibles y sin dilaciones. Se informará también a los titulares cuando se vean involucrados datos de NNA, datos sensibles o a obligaciones de carácter económico, financiero, bancario o comercial.

Colombia: Se debe reportar a la SIC a más tardar dentro de los 15 días hábiles siguientes al momento en el que se detecten los incidentes. Ahora bien, no es obligatorio, pero sí una buena práctica el comunicar a los titulares de la información.

06. ¿Se debe contar con un Registro de Actividades de tratamiento ("RAT")?

Chile: No es obligatorio contar con un RAT. Sin embargo, en caso de que se elabore un Modelo de Prevención de Infracciones, es necesario identificar aquellas actividades o procesos en que se puede generar o incrementar un riesgo de comisión de infracciones. Sin embargo, se recomienda siempre elaborar un RAT ya que actúa como una medida de control de la información al interior de la organización.

Colombia: No se establece ninguna regulación respecto el RAT. Sin embargo, la regulación sí exige el registro de las bases de datos en el Registro Nacional de Bases de Datos (RNBD) administrado por la SIC.

08. Evaluaciones de impacto en el tratamiento de datos personales ("EIPD")

Chile: Se exige una EIPD en caso de que el tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, produzca un alto riesgo para los derechos de las personas. Se publicará, por parte de la AGPD, tanto un listado de actividades de tratamiento que requerirán una EIPD como orientaciones mínimas para realizarla.

Colombia: No se encuentran reglamentadas de manera expresa las EIPD. Sin embargo, la SIC las reconoce como una medida adecuada para demostrar el cumplimiento del principio de responsabilidad demostrada (responsabilidad proactiva).

CONCLUSIONES



Evite multas por incumplimiento:

Chile: Hasta 20.000 UTM (~USD 1.5 millones) o 4% de ingresos. Pueden triplicarse en caso de reiteración.

Colombia: Hasta 2.000 salarios mínimos mensuales legales vigentes al momento de la imposición de la norma. Puede incluir la suspensión, cierre temporal o cierre definitivo de las actividades.



Evite multas por incumplimiento:

Cumplir ya no es solo evitar multas: es acelerar negocios, expandir mercados y ganar la confianza de clientes e inversionistas. En ECIJA ponemos a tu disposición un equipo altamente especializado en estas materias.



¿Cómo te podemos ayudar?

- Diagnosticamos tu nivel de cumplimiento y cerramos brechas.
- Diseñamos Modelos de Prevención de Infracciones.
- Redactamos políticas y contratos alineados con las normas de Chile, Colombia y estándares globales.
- Te acompañamos en el día a día de tu operación.
- Actuamos ante las autoridades.
- Capacitamos a tu equipo.

ECIJA