

USO PÚBLICO | ENERO 2026

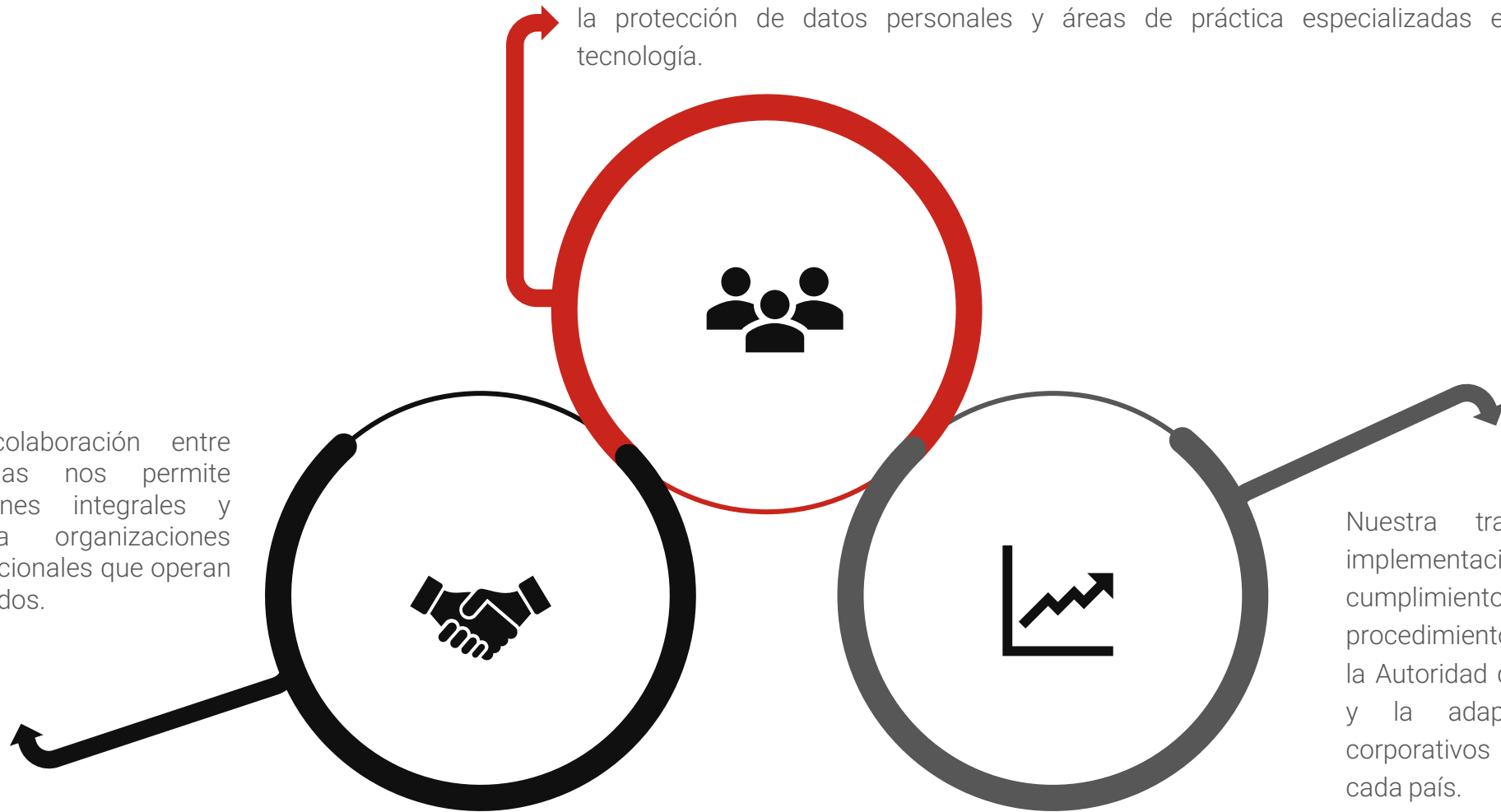
# Guía esencial en Protección de Datos Personales en Chile y República Dominicana

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 REPÚBLICA DOMINICANA EN LA 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.

**República Dominicana:** La Ley No. 172-13 tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados. La Constitución Dominicana garantiza el derecho a la intimidad y al honor personal, y establece los principios mínimos para el tratamiento de datos en su artículo 44.

## 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.

**República Dominicana:** Se reconocen los derechos **ARCO**: Acceso, Rectificación, Cancelación y Oposición. Además, se permite el derecho a indemnización en caso de sufrir daños y perjuicios y de ejercer la acción judicial de hábeas data. Los responsables de datos deberán garantizar el pleno y efectivo ejercicio de los derechos.

## 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.

**República Dominicana:** Se deberán cumplir con los principios y obligaciones determinadas en la normativa como son el deber de secreto del responsable, adoptar medidas de seguridad necesarias para salvaguardar la información y utilizar los datos para los fines para los cuales fueron recolectados, entre otros.

## 04. ¿Cómo se deben tratar los datos sensibles?

**Chile:** Sólo pueden tratarse con el consentimiento expreso del titular el cual debe ser otorgado de forma escrita, verbal o por medios tecnológicos. Existen otras excepciones como es que sean datos públicos, sean actividades realizadas por una entidad sin fines de lucro, para salvaguardar la vida, para formular una defensa jurídica, o en cumplimiento de una obligación legal.

**República Dominicana:** Sólo con el consentimiento expreso y por escrito del titular se podrán tratar datos sensibles. Se exceptúan los datos mantenidos por partidos políticos, sindicatos, y entidades sin fines de lucro cuya finalidad sea política, filosófica, religiosa o sindical. Podrán tratarse datos sensibles en la medida que sean necesarios para la prevención, asistencia o tratamiento de salud.

# CHILE Y REPÚBLICA DOMINICANA EN LA PROTECCIÓN DE DATOS PERSONALES

## 05. Encargados de tratamiento de datos personales

**Chile:** El tratamiento se puede realizar por medio de 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.

**República Dominicana:** El encargado de tratamiento puede ser un tercero mandatario conforme a las instrucciones del responsable de tratamiento. No existen requerimientos expresos, pero recomendamos celebrar un contrato en el que se establezca el objeto del encargo, duración, finalidad, tipo de datos tratados, categorías de los titulares y derechos y obligaciones de las partes.

## 07. Notificación de violaciones de seguridad de datos personales

**Chile:** Se debe reportar a la Agencia de Protección de Datos Personales (“APDP”) por los medios más expeditos posibles y sin dilaciones. Se informará también a los titulares cuando se vean involucrados datos de niños, niñas o adolescentes, datos sensibles o sean datos relativos a obligaciones de carácter económico, financiero, bancario o comercial.

**República Dominicana:** La normativa actual no define una entidad a la cual notificar las brechas de seguridad que expongan datos personales. De hecho, actualmente no existe una entidad independiente para la protección de datos personales – tipo APDP – en la República Dominicana.

## 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 en que se puede generar o incrementar un riesgo de comisión de infracciones. A pesar de lo anterior, se recomienda siempre elaborar un RAT ya que actúa como una medida de control de la información al interior de la organización.

**República Dominicana:** La normativa no regula el RAT. Sin embargo, se recomienda contar con uno ya que permite monitorear y supervisar el tratamiento de datos dentro de las organizaciones, actuando de esa manera como una medida interna de control; especialmente para las Sociedades de Información Crediticia (SIC).

## 08. Evaluaciones de impacto en la protección 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 APDP, un listado de actividades de tratamiento que requerirán una EIPD y los correspondientes lineamientos mínimos para realizarla.

**República Dominicana:** La ley vigente no regula este asunto. Sin embargo, se recomienda realizar evaluaciones de impacto, de acuerdo con los estándares internacionales, en vistas a cumplir con la responsabilidad proactiva. De igual forma, es recomendable ante cualquier requerimiento regulatorio para transferencia internacional de datos personales en el cual la entidad dominicana es la cedente.

# CONCLUSIONES



## Evita multas por incumplimiento:

**Chile:** Hasta 20.000 UTM (~USD 1.500.000 aproximadamente) o 4% de ingresos. Este monto puede verse hasta triplicado en caso de reiteración.

**República Dominicana:** Hasta 150 salarios mínimos vigentes, sin perjuicio de las reparaciones que procedan por los daños y perjuicios de derecho común. De igual forma, las personas físicas podrán ser sancionadas con prisión correccional de seis meses a dos años. Con la entrada en vigor del Código Penal en el 2026, las personas jurídicas podrán ser responsables por el tipo penal de *"captación y uso no consentido de datos personales"*. No obstante, esta norma toma en cuenta la existencia de programas de prevención para la atenuación de la sanción.



## Beneficios del cumplimiento

**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, República Dominicana y estándares globales.
- Te acompañamos en el día a día de tu operación.
- Actuamos ante las autoridades.
- Capacitamos a tu equipo.

ECIJA