



Fundamentos y Gobernanza de la Protección de Datos

Seminario Protección de Datos en la Empresa
Cámara de Comercio de Santiago

Raúl Arrieta Cortés

Reflexiones Iniciales



Empoderamiento ciudadano

Transición hacia los derechos personales y mayor conciencia sobre la privacidad digital.

El camino hacia una verdadera protección de datos en Chile ha sido lento. Las empresas deben adaptarse a un nuevo paradigma centrado en las personas.



Demandas insatisfechas

Insuficiencia del marco actual para responder a las necesidades de protección de datos personales.



Evolución lenta

Letargo de más de 20 años en la actualización de la normativa de protección de datos.

Evolución Normativa: De la Ley 19.628 a la Ley 21.719

El marco regulatorio de protección de datos en Chile ha experimentado una transformación significativa a lo largo de más de dos décadas.

Ley 19.628 (1999)

Publicada en un contexto muy diferente al actual: sin redes sociales, sin economía de plataformas y sin inteligencia artificial aplicada masivamente.

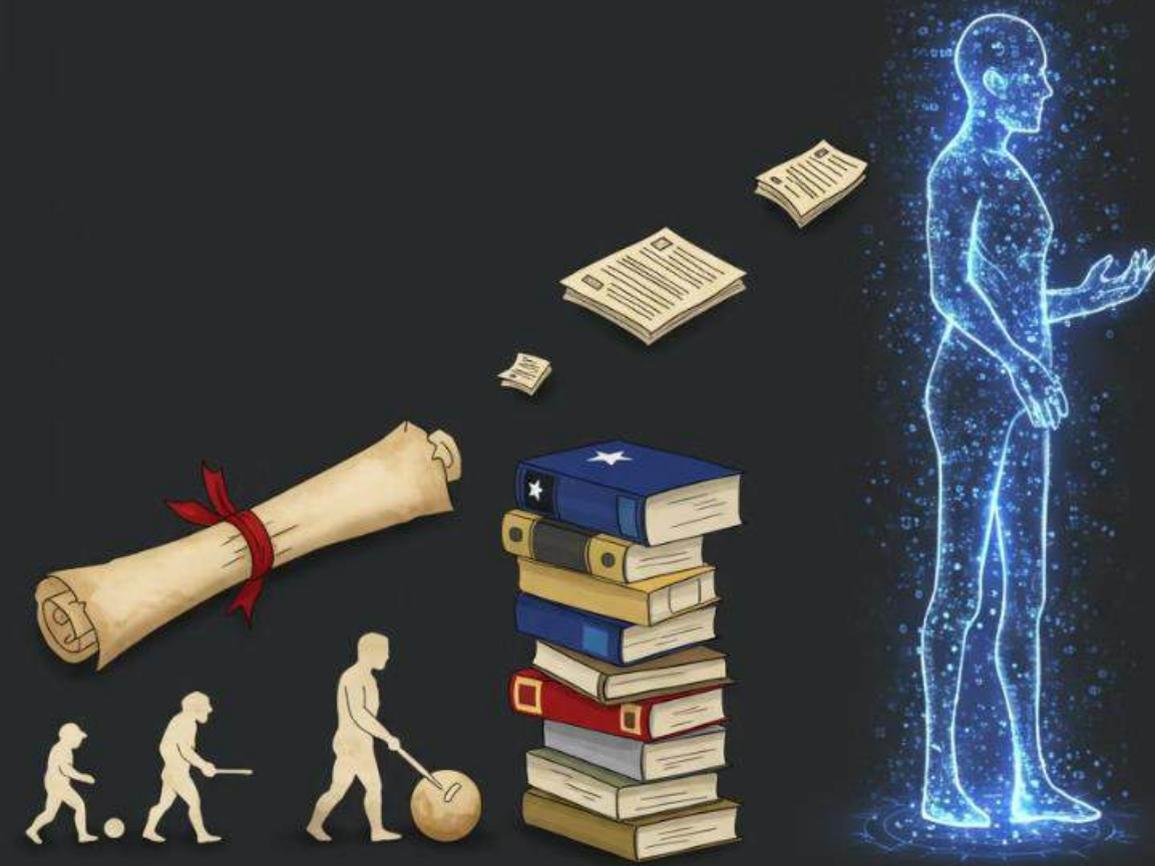
Ley 21.719 (2024)

Tras más de una década de debate legislativo, se promulga una ley que transforma completamente el marco normativo chileno.



Críticas y Obsolescencia

Falta de estándares robustos, ausencia de principios fundamentales, carencia de organismo fiscalizador autónomo y desalineación con marcos internacionales.



Características Principales de la Nueva Ley



Refuerzo de Principios y Derechos

Fortalece los principios de tratamiento y amplía los derechos de los titulares de datos personales.



Nuevas Figuras

Introduce la portabilidad de datos y el derecho a no ser objeto de decisiones automatizadas.



Sistema de Sanciones

Establece un sistema de sanciones graduadas para infracciones a la normativa.



Agencia Fiscalizadora

Creación de una Agencia de Protección de Datos Personales con facultades fiscalizadoras y sancionatorias.



Entrada en Vigencia Diferida



Publicación

13 de diciembre de 2024



Período de Adaptación

2 años para implementar cambios



Entrada en Vigor

1 de diciembre de 2026

Esta vacancia legal busca dar tiempo a los sectores público y privado para adaptarse al nuevo marco regulatorio. Las organizaciones tienen un plazo estratégico de dos años para diseñar políticas internas, implementar modelos de gobernanza, capacitar equipos y adaptar contratos, formularios y procesos.



Finalidad Principal

Regular la forma y condiciones en las cuales se efectúa el tratamiento y protección de los datos personales de las personas naturales.

Base Constitucional

Se fundamenta en el derecho constitucional a la protección de la vida privada.

Aplicación Universal

Se aplica a cualquier tratamiento de datos personales, tanto por parte de entidades públicas como privadas.

La ley establece un marco integral que busca equilibrar el uso legítimo de los datos con la protección efectiva de los derechos fundamentales de las personas, respetando siempre sus libertades en el entorno digital.

Ámbito Territorial de Aplicación

Responsable en Chile

Cuando el responsable o encargado está establecido en territorio chileno.

Aplicación por Contrato

Cuando el responsable no está en Chile, pero la legislación chilena le es aplicable por contrato o norma internacional.



Encargado Internacional

Cuando el encargado, sin importar su ubicación, trata datos en nombre de un responsable establecido en Chile.

Servicios Dirigidos a Chile

Cuando el tratamiento se dirige a personas ubicadas en Chile, aunque el responsable esté fuera del país.

Definiciones Esenciales

Dato Personal

Cualquier información vinculada o referida a una persona natural identificada o identificable.

Ejemplos: nombre, RUT, dirección, correo electrónico.

Dato Sensible

Aquellos datos que se refieren a características físicas o morales, salud, orientación sexual, creencias religiosas, opiniones políticas, entre otros.

Tratamiento de Datos

Toda operación que permita recolectar, almacenar, usar, comunicar, transferir o eliminar datos personales, sea automatizada o no.

Actores Principales en el Tratamiento



Responsable del Tratamiento

Persona natural o jurídica (pública o privada) que decide sobre los fines y medios del tratamiento de los datos. Es quien determina el "por qué" y el "cómo" se utilizarán los datos personales.



Encargado del Tratamiento

Persona natural o jurídica que trata los datos personales por cuenta del responsable, siguiendo sus instrucciones. Actúa como un prestador de servicios que procesa la información según las directrices recibidas.



Titular de los Datos

Persona natural a quien pertenecen los datos personales objeto de tratamiento. Es el sujeto de protección de la ley y quien puede ejercer los derechos que ésta reconoce.

Principios Rectores del Tratamiento

Licitud y Lealtad

Los datos deben ser tratados conforme a la ley y de manera honesta.

Transparencia

El titular debe conocer qué datos se tratan y con qué finalidad.

Seguridad

Protección contra accesos no autorizados, pérdidas o filtraciones.



Finalidad

Los datos deben recolectarse con fines específicos, explícitos y lícitos.

Proporcionalidad

Sólo deben tratarse los datos estrictamente necesarios.

Calidad

Los datos deben ser exactos, completos y actualizados.



Ejemplos Prácticos de los Principios

Principio	Ejemplo de Cumplimiento	Ejemplo de Incumplimiento
Licitud y Lealtad	Obtener consentimiento explícito antes de recolectar datos	Recolectar datos ocultos mediante cookies no informadas
Finalidad	Usar el correo solo para enviar la factura solicitada	Enviar publicidad sin autorización al correo recolectado para facturación
Proporcionalidad	Solicitar solo nombre y correo para una newsletter	Pedir estado civil o religión para suscribirse a un boletín
Seguridad	Implementar cifrado y contraseñas robustas	Almacenar datos en sistemas sin protección adecuada

Derechos del Titular de los Datos



La Ley 21.719 reconoce un conjunto amplio de derechos a los titulares de datos personales, fortaleciendo su capacidad de control sobre el tratamiento de su información. Estos derechos, conocidos comúnmente como derechos ARCO (Acceso, Rectificación, Cancelación/Supresión y Oposición), se amplían en esta ley e incluyen nuevas facultades.

Derecho de Acceso

Definición

Permite al titular saber si sus datos están siendo tratados y conocer el detalle de dicho tratamiento.

Información que se puede solicitar

- Finalidades del tratamiento
- Categorías de datos tratados
- Destinatarios de los datos
- Plazo de conservación

Forma de ejercicio

Mediante solicitud directa al responsable, quien debe responder en un plazo máximo de 30 días corridos, prorrogables por otros 30 días una sola vez.



Derechos de Control sobre los Datos

Rectificación

Permite corregir datos inexactos, incompletos o desactualizados. Por ejemplo, actualizar una dirección de domicilio o corregir errores en el nombre.

Supresión

También conocido como 'derecho al olvido', permite eliminar los datos cuando ya no son necesarios o el tratamiento es ilícito. Aplica cuando la finalidad para la que se recolectaron ya se cumplió.

Oposición

Permite al titular negarse al tratamiento de sus datos en ciertas circunstancias, especialmente en marketing directo o cuando se basa en intereses legítimos del responsable.

Nuevos Derechos Digitales



Portabilidad

Permite al titular obtener una copia de sus datos en formato estructurado y transferirlos a otro responsable. Facilita el cambio entre proveedores de servicios sin perder la información personal.



Bloqueo

Permite suspender temporalmente el tratamiento mientras se resuelve una solicitud de rectificación, oposición o supresión. El responsable debe aplicarlo en un plazo de 2 días hábiles.

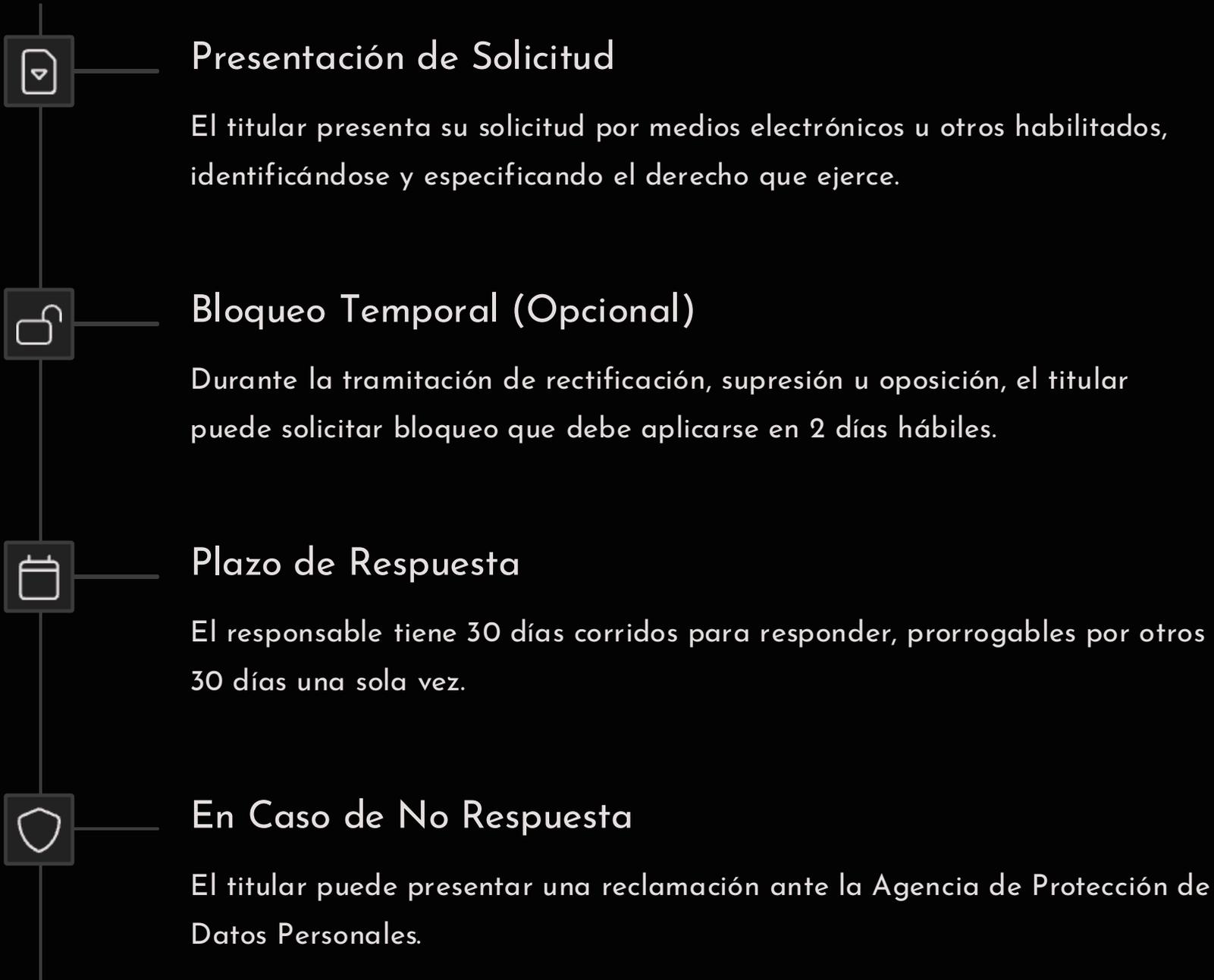


No Decisiones Automatizadas

Derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos, incluyendo perfiles, que produzcan efectos jurídicos o afecten significativamente.



Ejercicio de Derechos y Plazos



Data Fights Frquest

Obligaciones de Transparencia

1 Política de Tratamiento

Publicar su política de tratamiento de datos y mantenerla permanentemente disponible en un lenguaje claro y accesible.

2 Identificación Clara

Identificar claramente al responsable, su representante legal y datos de contacto para facilitar el ejercicio de derechos.

3 Información sobre Finalidades

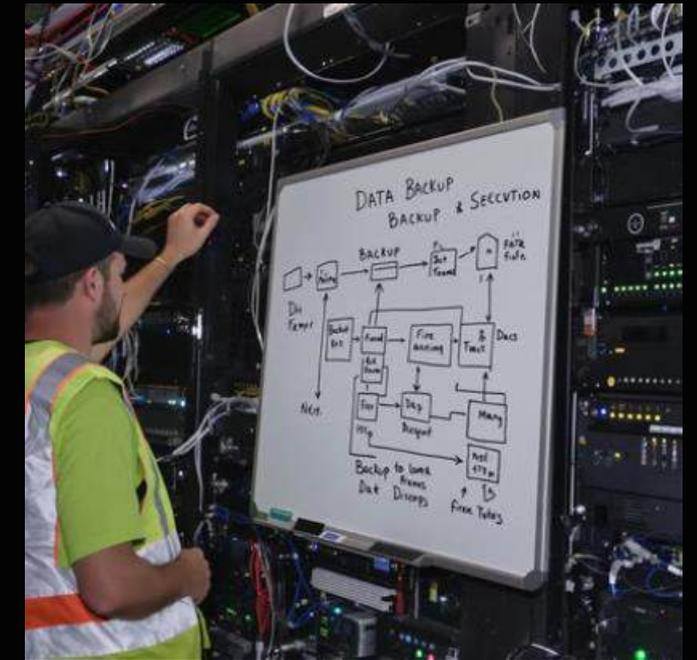
Comunicar de manera explícita los propósitos del tratamiento y los destinatarios de los datos.

4 Canales de Atención

Establecer mecanismos simples y accesibles para que los titulares puedan ejercer sus derechos.



Medidas de Seguridad



El responsable debe aplicar medidas técnicas y organizativas adecuadas para proteger los datos desde el diseño y por defecto. Estas incluyen mecanismos como cifrado, seudonimización, controles de acceso y capacidad de restauración ante incidentes. La seguridad debe ser proporcional al riesgo y considerar el estado de la técnica y los costos de implementación.

Notificación de Vulneraciones de Seguridad



Detección del Incidente

Identificación de una brecha de seguridad que afecte datos personales.



Evaluación de Riesgos

Análisis del impacto potencial para los derechos de los titulares.



Notificación a la Agencia

Comunicación a la autoridad en un plazo máximo establecido.



Notificación a Titulares

En casos de alto riesgo, informar directamente a los afectados.

Gobernanza de Datos Personales

Políticas y Procedimientos

Documentos formales que establecen directrices y procesos

Mejora Continua

Actualización basada en resultados y cambios normativos



Roles y Responsabilidades

Asignación clara de funciones en la organización

Controles y Auditorías

Verificación periódica del cumplimiento

Evaluación de Impacto a la Protección de Datos

Identificación de Tratamientos de Alto Riesgo

Determinar qué operaciones de tratamiento pueden generar un riesgo elevado para los derechos de los titulares.

Evaluación de Riesgos

Identificar amenazas, estimar su probabilidad e impacto, y analizar vulnerabilidades.

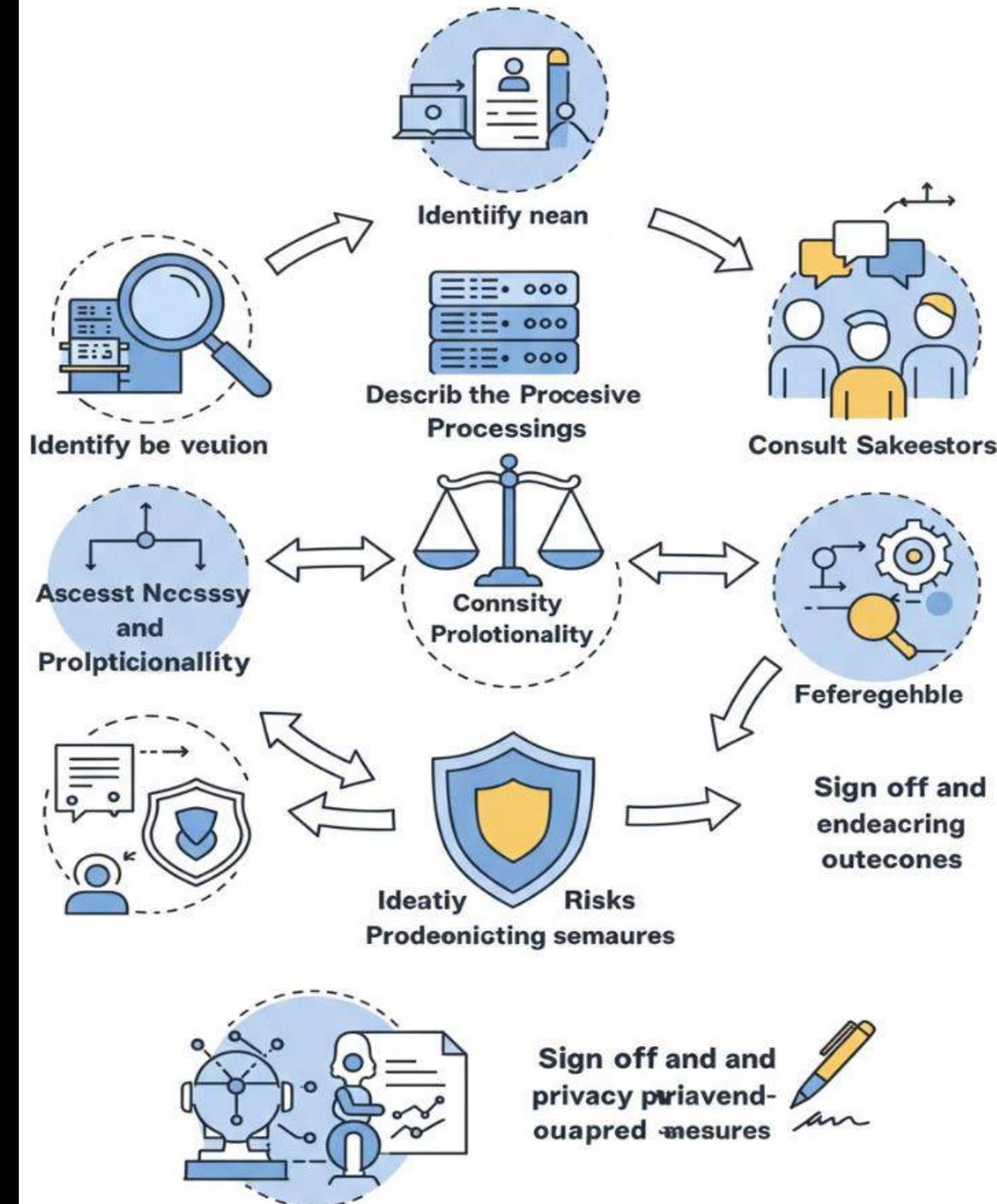
Descripción Sistemática del Tratamiento

Documentar finalidades, categorías de datos, flujos de información y medidas de seguridad existentes.

Definición de Medidas de Mitigación

Establecer controles adicionales para reducir los riesgos identificados a un nivel aceptable.

Data Protection Impact Assessment



Delegado de Protección de Datos



Perfil y Cualificaciones

Debe tener autonomía y contar con conocimientos técnicos adecuados en materia de protección de datos y normativa aplicable. Puede ser interno o externo a la organización.



Funciones Principales

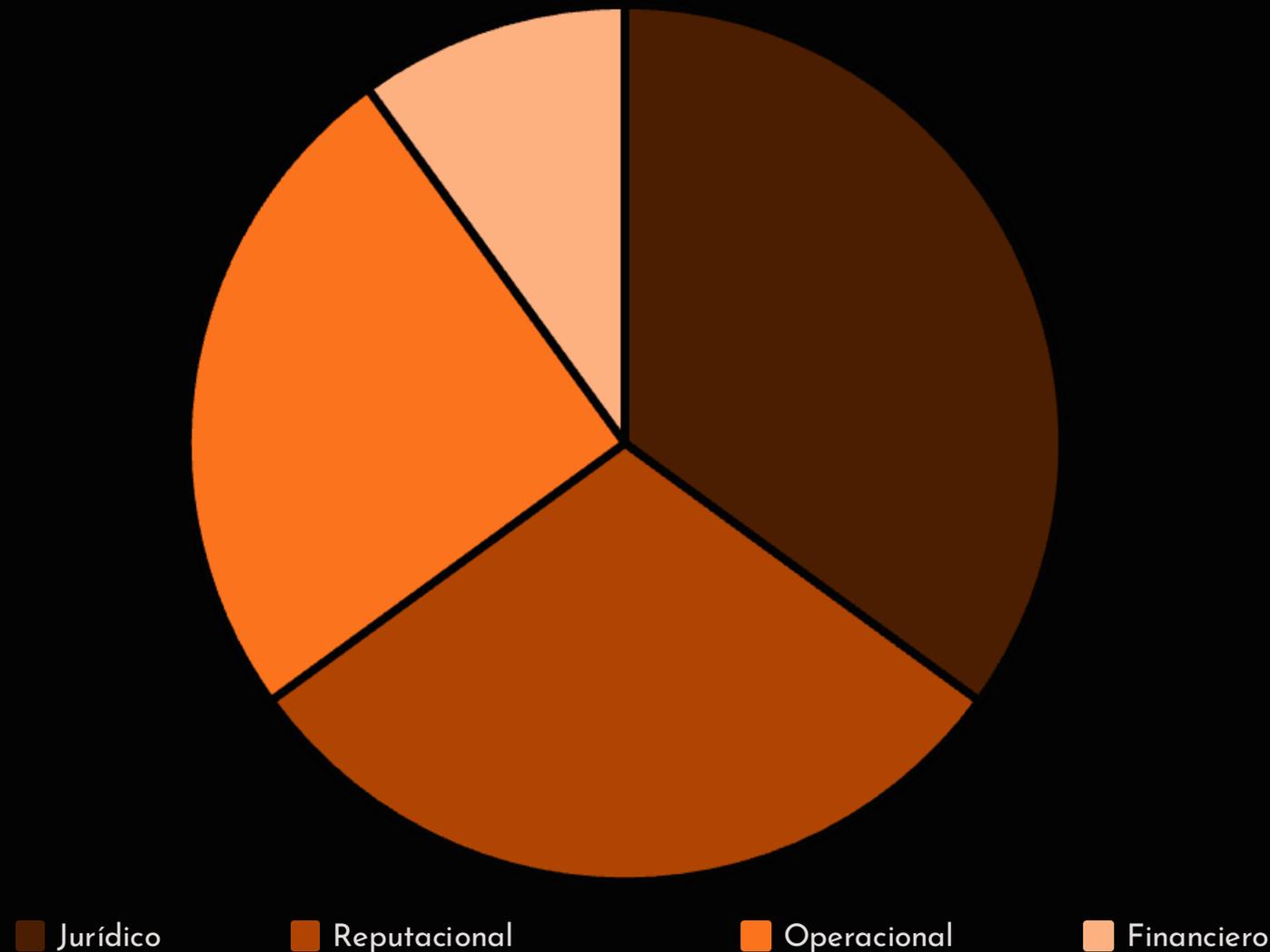
Supervisar el cumplimiento normativo, asesorar en el diseño de medidas, cooperar con la Agencia, y servir de enlace con los titulares para el ejercicio de sus derechos.



Flexibilidad Organizativa

En empresas más pequeñas, esta función puede ser asumida por el propio dueño o la máxima autoridad. En grupos empresariales, puede existir un delegado común.

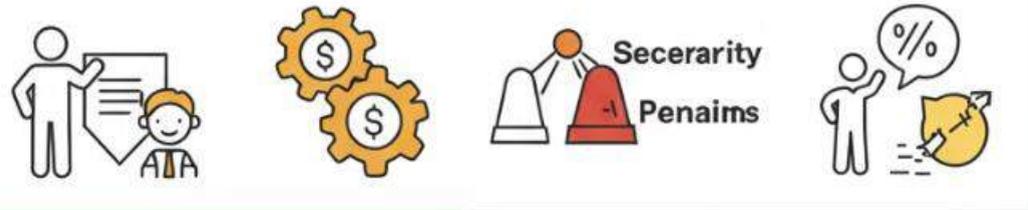
Gestión de Riesgos en Protección de Datos



Una gestión anticipada de los riesgos de privacidad permite a las organizaciones evitar sanciones, mantener la confianza de clientes y usuarios, y mejorar su reputación. El cumplimiento normativo en esta materia se ha convertido en un factor crítico para el acceso a mercados internacionales, especialmente en entornos donde se exige un nivel adecuado de protección.

Regulatory on Compliance Level Severity Levels

Penitition Penintire



Cofertive Fenipistios

Peolyatrye Tecaive



Praises



Fittios 1917

Fittios: 1750

Fittios: 1207

Fittios 4505

Lorem ipsum dolm amet, cingeh t amet miso regand diule amcam ean dious

Lorem ipsum dolm amet, cingeh t amet miso regand diule amgam ean dious

Lorem ipsum dolm amet, cingeh t amet miso regand diule amcam ean dious

Lorem ipsum dolm amet, cingeh t amet miso regand diule amgam ean dious



Conalo



Level



Ject

Civel



Level

Infracciones y Sanciones

5.000

10.000

UTM Leves

UTM Graves

Amonestación escrita y multa.
Incumplimientos menores de obligaciones formales.

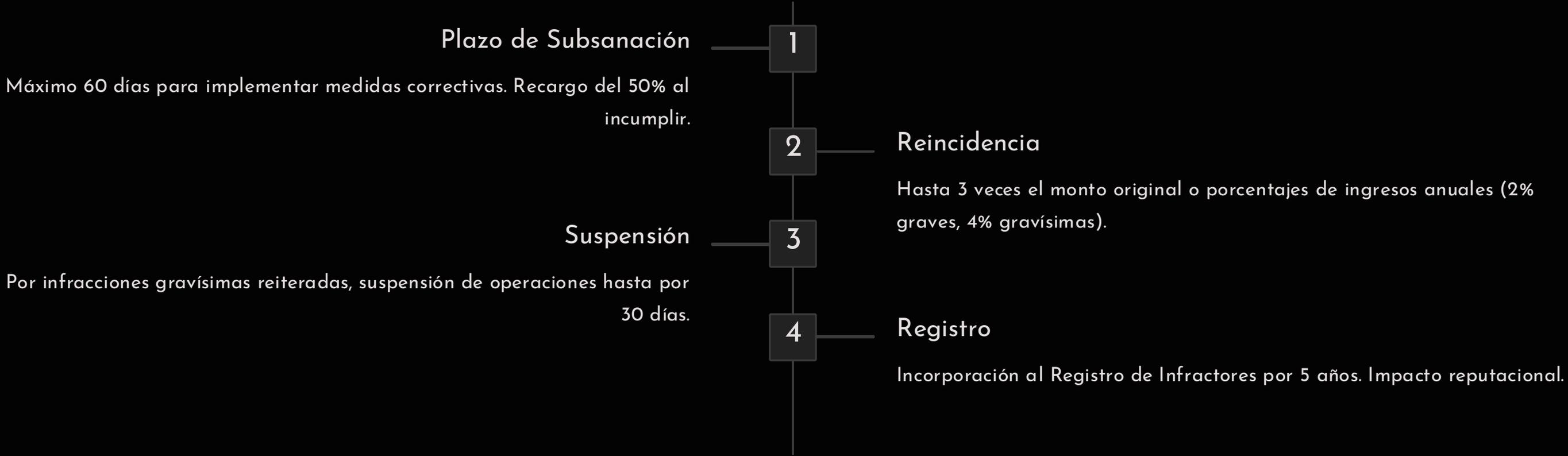
Tratamiento sin consentimiento o fuera de la finalidad autorizada.

20.000

UTM Gravísimas

Vulneraciones severas como uso fraudulento o negligente de datos sensibles.

Sistema Sancionatorio Reforzado



Raúl Arrieta Cortés

raul.arrieta@ga-abogados.cl

+56 2 2638 1527

www.ga-abogados.cl

Descarga nuestra **Guía Práctica para adecuarse a la Nueva Normativa de Protección de Datos**



Guía Práctica para adecuarse a la Nueva Normativa de Protección de Datos



GA.ABOGADOS

GA.ABOGADOS