LEY 21.719

COMPLIANCE Y PROTECCIÓN DE DATOS PERSONALES

iSentinel
Protegemos el éxito de su negocio

Av. La Divisa 0340. San Bernardo.
Santiago Chile.
Fono: +569 5316 7879.
Correo: info@isentinel.cl.
www.isentinel.cl

CONTENIDO

01 LA LEY

El 13 de diciembre de 2024 se publicó la Ley 21.719 que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

Una nueva herramienta para resguardar la privacidad de la ciudadanía. La normativa busca regular cómo empresas, instituciones y organismos públicos manejan la información, estableciendo reglas claras para así evitar abusos y proteger derechos básicos de la población.

La legislación establece una serie de derechos fundamentales que permiten a las personas solicitar acceso a sus datos, exigir su corrección en caso de errores o cambios y requerir su eliminación cuando se considere que estos ya no sean necesarios.

02 ASPECTOS PRINCIPALES

CONSENTIMIENTO

CONSENTIMIENTO CLARO Y DERECHOS DE LAS PERSONAS

Antes de usar Datos Personales, las empresas deberán pedir permiso de manera clara, informada y explícita.

PROTECCIÓN DE DATOS SENSIBLES

PROTECCIÓN REFORZADA DE DATOS SENSIBLES

Información de salud, datos biométricos, preferencias personales, se consideran datos sensibles. Por lo que no se pueden usar sin autorización específica.

CREACIÓN DE APD

NUEVA AGENCIA DE PROTECIÓN DE DATOS

Entidad especial para supervisar y sancionar a quienes no cumplan con las normas.

Esta Ley se alinea con estándares internacionales (similar al GDPR europeo) y eleva el nivel de protección hasta ahora existente, impactando a sectores sensibles como financiero, salud, retail, marketing, telecomunicaciones, entre otros.

CONTEXTO NORMATIVO Y ALCANCE DE LA LEY

AMPLIO ÁMBITO DE APLICACIÓN

Cubre a personas naturales y jurídicas, públicas y privadas, que traten datos personales de personas en Chile.

AUTORIDAD DE CONTROL

Creación de la Agencia de **Protección de Datos Personales** con potestades de fiscalización, sanción y emisión de instrucciones.

DERECHOS DE LOS TITULARES

Acceso, rectificación, supresión, oposición, portabilidad, bloqueo temporal y protección frente a decisiones automatizadas.

PRINCIPIOS CLAVES

Licitud, finalidad, proporcionalidad, calidad, responsabilidad, seguridad, transparencia e información, y confidencialidad.

IMPLICANCIAS

03 PARA EMPRESAS Y ORGANIZACIONES

Ajustes Internos Necesarios:

1. **Consentimiento y Base Legal** — Toda recolección y tratamiento de datos deberá contar con consentimiento libre, informado y específico, o con otra base jurídica prevista en la Ley.

2. **Obligaciones de Información y Transparencia** — Se debe informar al titular sobre las finalidades del tratamiento, la identidad del responsable, el plazo de conservación de datos, la posibilidad de ejercer derechos, etc.

3. **Nuevos Procedimientos** — Las empresas deberán implementar mecanismos para el ejercicio de derechos (acceso, rectificación, supresión, oposición, etc.) de forma expedita y gratuita, al menos trimestralmente.

4. **Reportar Incidentes de Seguridad** — Ante vulneraciones que afecten datos personales, se debe notificar a la Agencia y, en algunos casos, a los titulares afectados.

5. **Designación de Delegados de Protección de Datos** — La Ley incentiva la adopción de modelos de prevención y el nombramiento de un delegado con autonomía y facultades suficientes.

IMPLICANCIAS

PARA EMPRESAS Y ORGANIZACIONES

Sanciones

1

20.000 UTM

LAS SANCIONES PUEDEN LLEGAR HASTA 20.000 UTM (O INCLUSO PORCENTAJES DE INGRESOS EN CASO DE REINCIDENCIA EN EMPRESAS DE MAYOR TAMAÑO), GENERANDO UN IMPACTO FINANCIERO RELEVANTE.

2

DAÑO REPUTACIONAL Y LA PÉRDIDA DE CONFIANZA POR PARTE DE CLIENTES Y SOCIOS.

04 REQUERIMIENTOS TÉCNICOS Y ORGANIZACIONALES

QUE LAS EMPRESAS DEBERÁN CUMPLIR

SEGURIDAD DE LA INFORMACIÓN

Implementar medidas técnicas y organizativas acordes con el estado de la técnica, incluyendo el cifrado de datos tanto en reposo como en tránsito, la seudonimización, controles de acceso adecuados, auditorías periódicas y planes de contingencia que garanticen la resiliencia frente a incidentes de seguridad.

GESTIÓN DE PROVEEDORES Y TERCEROS

Velar porque socios, proveedores y otros terceros cumplan con las mismas obligaciones legales, formalizando contratos con cláusulas apropiadas que reflejen los estándares de protección de datos exigidos.

GOBERNANZA DE DATOS

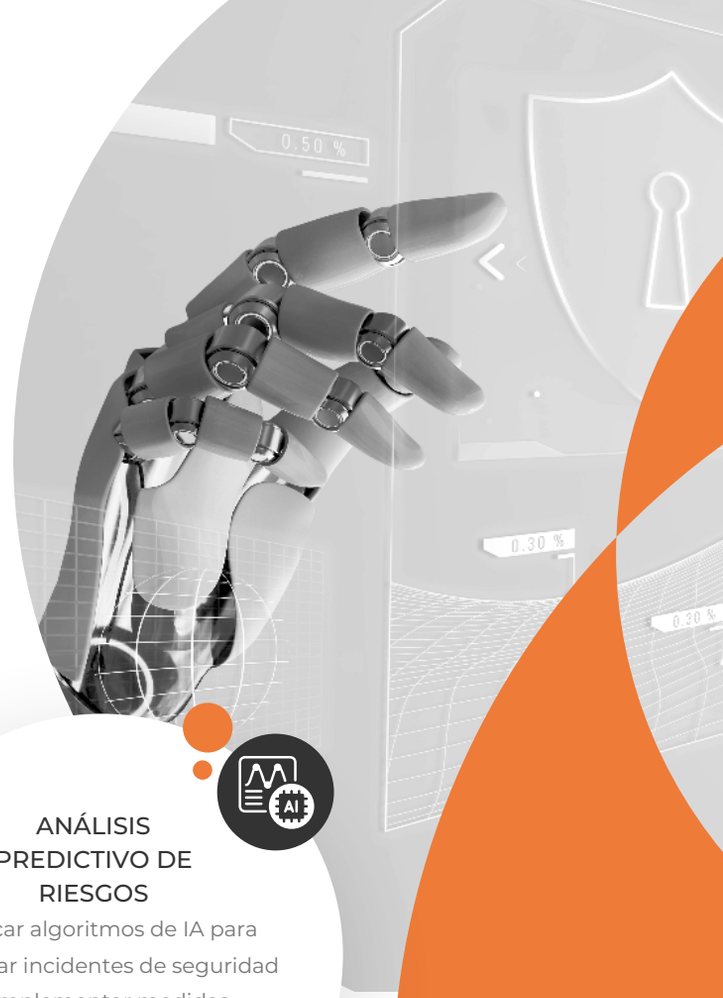
Definir políticas y procedimientos internos claros, establecer roles y responsabilidades bien delineados y asegurar la adecuada gestión del ciclo de vida de los datos personales.

CAPACITACIÓN INTERNA

Formar y concientizar de manera continua al personal en materia de protección de datos, difundir las políticas internas, garantizar la correcta respuesta ante incidentes y promover el conocimiento de los derechos de los titulares.

IA Y CIBERSEGURIDAD

ROL DE LA IA GENERATIVA Y LA CIBERSEGURIDAD EN EL CUMPLIMIENTO



IA GENERATIVA

IDENTIFICACIÓN DE DATOS SENSIBLES

Herramientas de IA pueden revisar grandes volúmenes de información para detectar datos sensibles o personales, optimizando la adecuación a la normativa.

AUTOMATIZACIÓN DE PROCESOS DE CUMPLIMIENTO

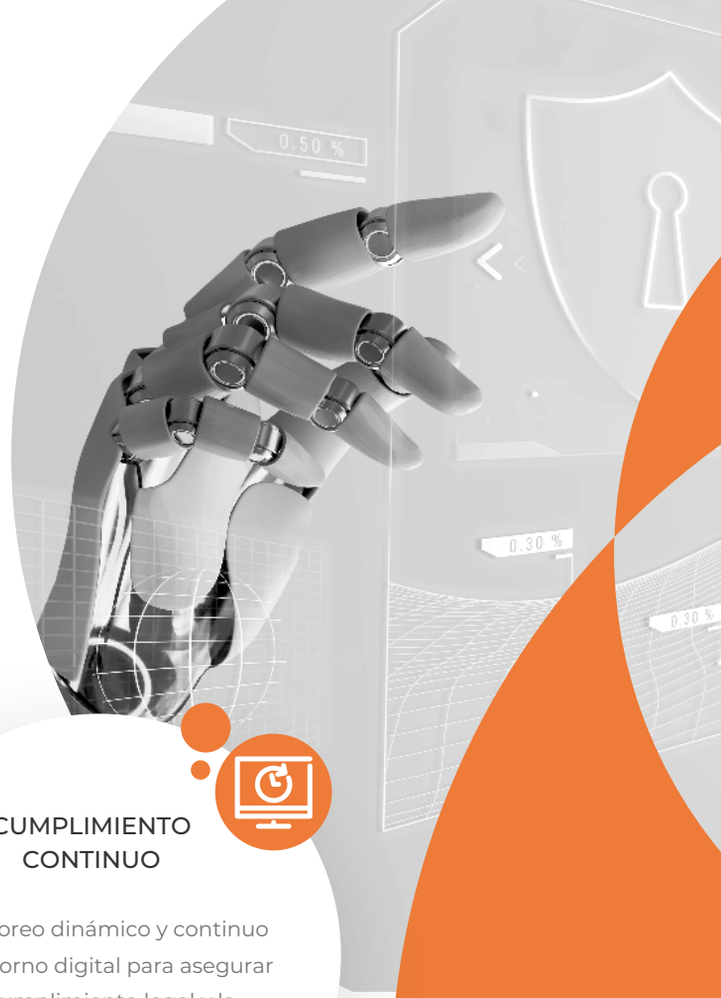
Uso de chatbots o asistentes virtuales para atender solicitudes de titulares, responder consultas internas, o recomendar mejores prácticas a partir de las regulaciones.

ANÁLISIS PREDICTIVO DE RIESGOS

Aplicar algoritmos de IA para anticipar incidentes de seguridad e implementar medidas proactivas.

IA Y CIBERSEGURIDAD

ROL DE LA IA GENERATIVA Y LA CIBERSEGURIDAD EN EL CUMPLIMIENTO



CIBERSEGURIDAD AVANZADA

DETECCIÓN DE AMENAZAS

Herramientas de ciberseguridad basadas en IA para identificar patrones anómalos, accesos no autorizados y brechas antes de que causen daños mayores.

RESPUESTA A INCIDENTES

Automatización de protocolos para contener incidentes, recuperar datos, y reportar a las autoridades en los plazos establecidos.

CUMPLIMIENTO CONTINUO

Monitoreo dinámico y continuo del entorno digital para asegurar el cumplimiento legal y la integridad de los datos.

QUÉ HACER PARA CUMPLIR

05 ETAPAS Y PRIORIDADES

1 DIAGNÓSTICO Y GAP ANALYSIS

- IDENTIFICACIÓN DEL ESTADO ACTUAL DEL TRATAMIENTO DE DATOS.
- DETECCIÓN DE BRECHAS NORMATIVAS.
- PRIORIZACIÓN DE RIESGOS MÁS CRÍTICOS.

2 DISEÑO DE POLÍTICAS Y PROCEDIMIENTOS

- ACTUALIZACIÓN DE POLÍTICAS DE PRIVACIDAD, AVISOS LEGALES Y CONSENTIMIENTOS.
- DEFINICIÓN DE FLUJOS PARA EL EJERCICIO DE DERECHOS DE LOS TITULARES.
- ESTABLECIMIENTO DE PROTOCOLOS DE RESPUESTA A INCIDENTES.

3 IMPLEMENTACIÓN TECNOLÓGICA Y ORGANIZACIONAL

- ADOPCIÓN DE SISTEMAS DE CIFRADO, SEUDONIMIZACIÓN Y MONITOREO.
- CAPACITACIÓN DEL PERSONAL.
- ESTABLECIMIENTO DE CANALES DE COMUNICACIÓN CON EL TITULAR.

4 VERIFICACIÓN Y AUDITORÍA INTERNA

- EVALUACIÓN DE CUMPLIMIENTO A TRAVÉS DE PRUEBAS Y AUDITORÍAS.
- AJUSTES Y MEJORAS CONTINUAS.

5 CERTIFICACIÓN Y MEJORA CONTINUA

- OBTENCIÓN DE CERTIFICACIONES.
- MANTENCIÓN ACTUALIZADA DEL MODELO DE CUMPLIMIENTO.
- REVISIÓN PERIÓDICA ANTE CAMBIOS REGULATORIOS O TECNOLÓGICOS.

06 BUENAS PRÁCTICAS
QUÉ DEBEN HACER LAS EMPRESAS SEGÚN SU SECTOR

SECTOR FINANCIERO

Entidades que utilizan IA para análisis de crédito deberán reforzar medidas de privacidad y transparencia, especialmente frente a la elaboración de perfiles automatizados.

SECTOR SALUD

Mayor resguardo de datos sensibles de pacientes, controles estrictos en el acceso a historiales médicos y anonimización de datos para investigación.

RETAIL Y MARKETING

Depurar bases de datos, obtener consentimientos expresos y mejorar la calidad de la información, respetando los derechos de oposición y supresión.

07 PRÓXIMOS PASOS

01 **Iniciar Prontamente el Diagnóstico:**
Comprender el estado actual y las brechas.

02 **Buscar Asesoría Especializada:**
Contar con expertos en protección de datos, IA y ciberseguridad.

03 **Adoptar Soluciones Tecnológicas Adecuadas:**
Herramientas de IA generativa y monitoreo continuo de seguridad.

04 **Construir una Cultura Interna de Cumplimiento:**
Capacitar al personal y promover la responsabilidad colectiva.

CONCLUSIONES Y PRÓXIMOS PASOS

La nueva Ley de Protección de Datos Personales en Chile representa un desafío y a la vez una oportunidad estratégica para las organizaciones. Cumplir con la normativa no se trata solo de evitar sanciones, sino de construir confianza con clientes, usuarios y partners. El cumplimiento posiciona a las empresas como actores responsables y sostenibles en el ecosistema digital.

Las empresas cuentan con un plazo de transición para ajustarse. Sin embargo, postergar las acciones corre el riesgo de no llegar a tiempo al plazo legal.

CONTÁCTENOS

AV. LA DIVISA 0340. SAN BERNARDO.
SANTIAGO CHILE.
FONO: +569 5316 7879.
CORREO: INFO@ISENTINEL.CL.
WWW.ISENTINEL.CL

iSentinel
Protegemos el éxito de su negocio

Nuestro equipo de profesionales en ISENTINEL está preparado para asesorarlo y ayudarle a entender cómo la ley 21.719 de Protección de Datos Personales puede impactar a su empresa y qué pasos debe seguir para cumplir con sus requisitos.