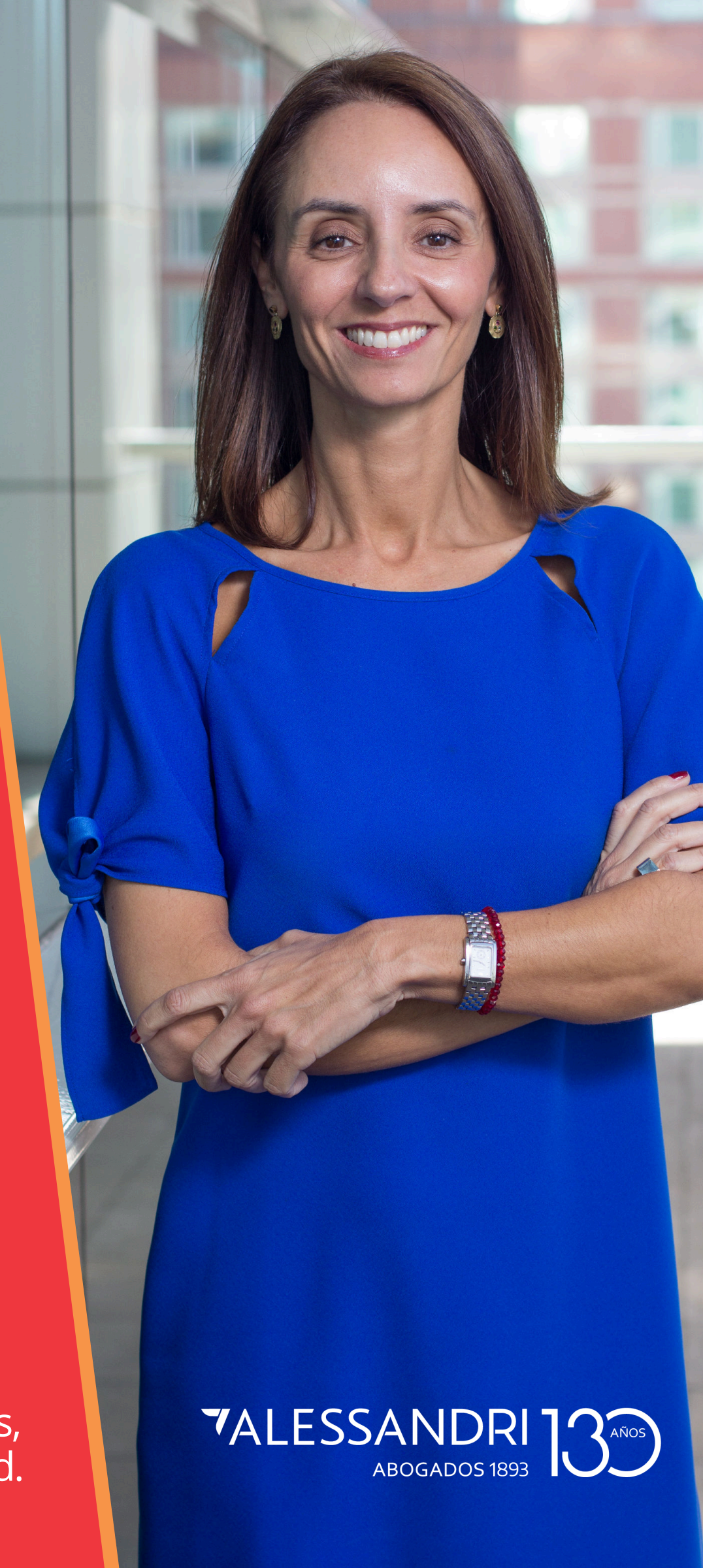
Ley de **datos personales**

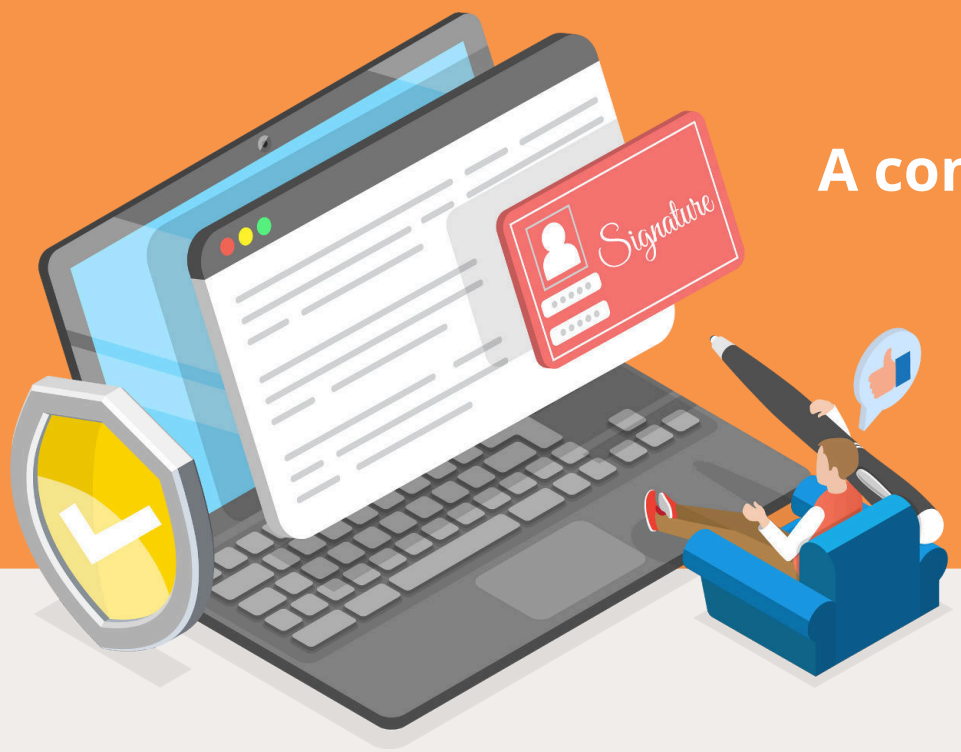
Claves para su implementación en las empresas



Por Macarena Gatica, socia Alessandri Abogados, experta en protección de datos y ciberseguridad.

Luego de más de siete años de tramitación legislativa, el proyecto de ley de datos personales ha sido despachado a ley. Ahora corresponde el examen de constitucionalidad que realiza el Tribunal Constitucional.

A continuación podrás conocer más detalle del nuevo cumplimiento normativo y de qué manera afectará a las organizaciones.

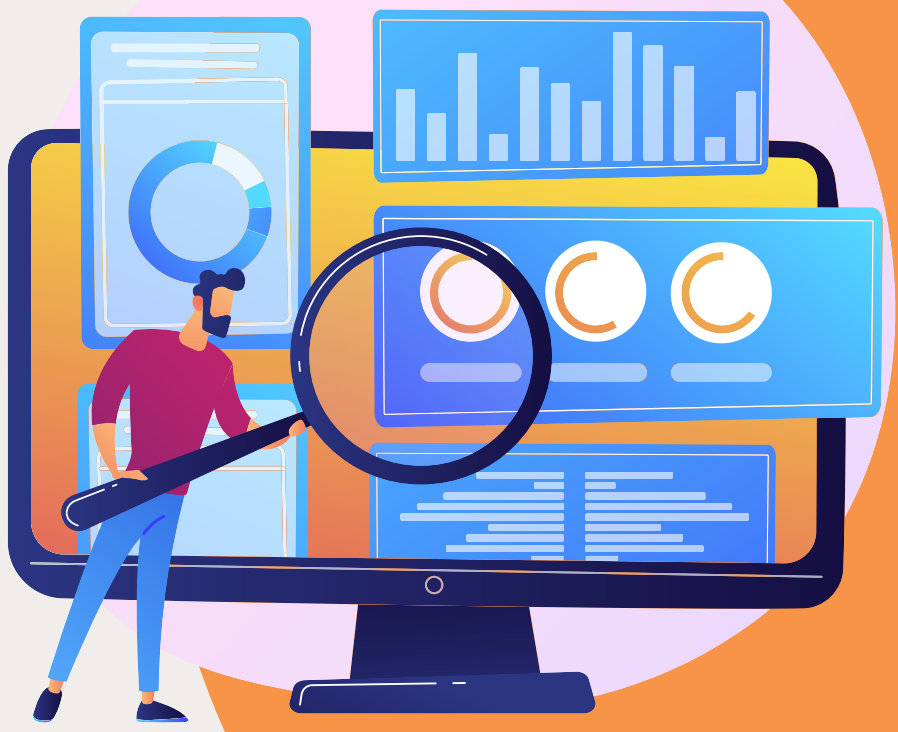


¿Cuándo entra en vigencia la nueva Ley de Datos Personales?

Luego de 24 meses desde la publicación de la nueva Ley.

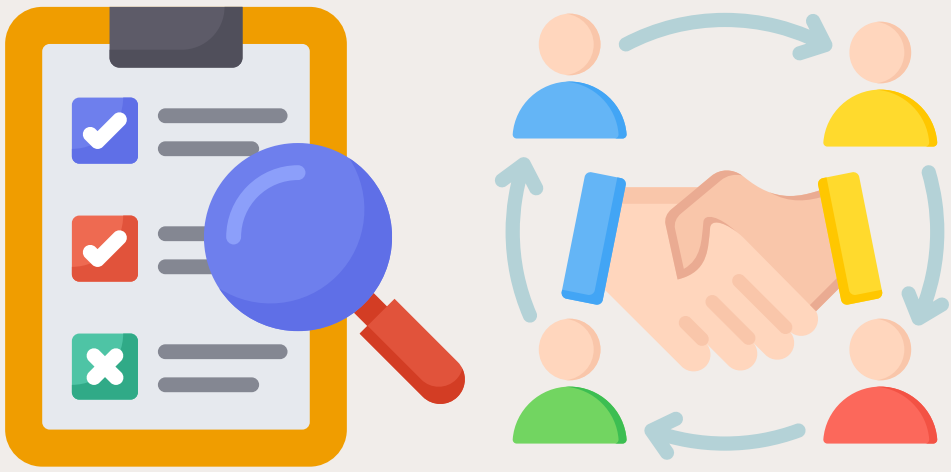
¿Qué deben hacer las empresas para prepararse?

- Realizar auditorías de los procesos que involucran tratamiento de datos.
- Determinar el nivel de cumplimiento de la empresa respecto de la nueva legislación, así como el nivel de exposición a riesgos normativos.
- Identificar bases de datos y depurarlas conforme al principio de proporcionalidad.
- Revisar y actualizar políticas de privacidad.
- Identificar bajo qué bases de licitud la empresa puede tratar los datos personales que actualmente procesa.
- Analizar los proveedores que intervengan en el tratamiento de datos que realiza la empresa. Ellos son encargados del tratamiento de datos y deben cumplir el estándar definido por la empresa.
- No olvidar el tratamiento de datos personales que el empleador hace de sus trabajadores y el asociado a cumplimiento, estos también requieren adecuación.



¿Qué medidas de seguridad deben implementar las empresas?

- Adoptar medidas técnicas y organizativas adecuadas, tales como accesos y controles, con el objeto de limitar el acceso a la información de acuerdo con el rol de cada trabajador, contar con medidas tecnológicas tales como firewalls y antivirus, suscribir acuerdos de tratamiento de datos, seudo anonimizar, siempre que sea posible, de acuerdo con el tratamiento de datos que se realiza, entre otras.
- Determinar la idoneidad de los proveedores.
- Determinar controles y realizar auditorías con el objeto de velar por el cumplimiento de estos y en su caso implementar mejoras.



¿Cómo deben gestionar las empresas los riesgos asociados a la protección de datos?

- Adoptar medidas tendientes a prevenir infracciones, es decir, una debida diligencia. Lo cual se logra mediante un sistema de gestión de riesgo.
- Capacitar en forma periódica al directorio y a todos los trabajadores de la empresa.
- Realizar Evaluaciones de Impacto en Protección de Datos Personales, también conocidas como PIA (Privacy Impact Assessments), que permiten medir y mitigar los riesgos asociados a una iniciativa que involucra tratamiento de datos personales.
- Crear una matriz de riesgo.
- Establecer controles y auditar su cumplimiento y mejoras.
- Construir una cultura de evidencia.
- Establecer planes de respuesta a incidentes que permitan trazar un plan de acción en caso de que los datos personales se vean vulnerados.

¿Qué papel juega la Agencia de Protección de Datos Personales?

- La Agencia de Protección de Datos Personales es el órgano encargado de velar por el cumplimiento de la ley. Conforme a ello contará con las siguientes facultades:
- Normativas: podrá impartir instrucciones y normas, e interpretar disposiciones legales y reglamentarias de datos personales.
- Fiscalizadoras: podrá auditar o requerir información a quienes traten datos personales.
- Sancionatorias: podrá imponer multas o exigiendo la suspensión del tratamiento de datos a quienes infrinjan la ley.
- Coordinadoras: se relacionará y colaborará con los órganos públicos e internacionales

¿Cómo deben adaptarse las empresas al nuevo modelo de opt-in?

- Revisar sus bases de datos actuales, distinguiendo cuales de ellas se tratan en virtud de la ley y en el consentimiento.
- Verificar que los consentimientos cumplan con el estándar actual.
- Revisar qué es lo que será necesario adecuar conforme a la nueva regulación. Por ejemplo, aplicar granularidad basado en el consentimiento libre.
- Implementar políticas de privacidad y formularios de captura de consentimientos.
- Contar con un sistema que permita gestionar los consentimientos de acuerdo con las preferencias de los titulares de datos (consentimiento granular).
- Eliminar los datos que no cuenten con un consentimiento para ser tratados o que no se enmarquen en alguna de las otras bases de licitud establecidas por la ley.
- Tener presente que la nueva regulación modifica el regimiento de las fuentes de acceso público.

¿Qué debe contener un modelo de prevención de infracciones?

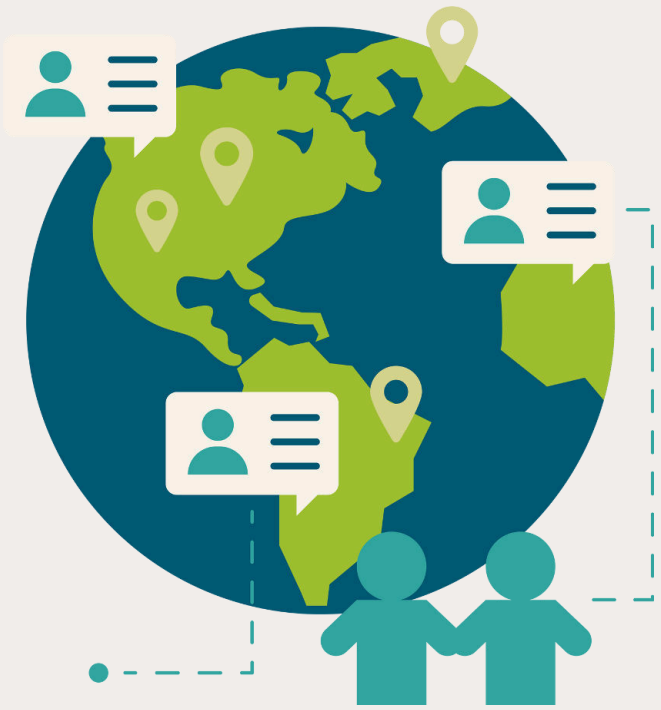
- Políticas y procedimientos claros que permitan a la empresa gestionar los riesgos asociados al tratamiento de datos personales. Mecanismos de monitoreo y control capaces de advertir riesgos en el tratamiento de datos y el establecimiento de medidas para mitigarlos.
- Programas de concienciación y formación continua que logren que los colaboradores estén en conocimiento de los estándares que exigen las normas sobre protección de datos.

¿Qué sanciones enfrentan las empresas por incumplimiento de la ley?

Principalmente las siguientes:

Tipo infracción	Multa
leves	amonestación escrita o multa de hasta **5.000** UTM
graves	multa de hasta **10.000** UTM
gravísimas	multa de hasta **20.000** UTM

- En caso de reincidencia, la Agencia podrá aplicar una multa de hasta tres veces el monto asignado a la infracción cometida. Si la reincidencia se refiere a infracciones graves o gravísimas de empresa de gran tamaño, existirá alternativamente la posibilidad de ser sancionado con el 2% o 4% de los ingresos anuales por ventas y servicios.
- Durante el primer año de vigencia de la ley las pymes no estarán afectas a multas, sino que solo a amonestaciones.
- Los titulares afectados podrán demandar la indemnización de los perjuicios sufridos. En relación con ello, el Sernac y las asociaciones de consumidores pueden ejercer acciones colectivas fundado en el daño moral difuso.
- Finalmente, y no por ello menos importante es el daño reputacional que puede sufrir una empresa al ser fiscalizado y condenado.



¿Cómo pueden las empresas manejar las transferencias internacionales de datos personales?

La ley establece que un país tiene niveles adecuados de protección de datos cuando cumple con estándares similares o superiores a los fijados en aquella. Uno de esos estándares es la existencia de garantías adecuadas como instrumentos, mecanismos, cláusulas con similares o mayores principios, derechos y garantías a las que ofrece la ley y que otorguen derechos exigibles y acciones legales efectivas a los titulares de los datos. Lo recomendable es comenzar identificando que flujos internacionales existen, jurisdicciones y medidas adicionales que se puedan implementar con el fin de proteger los datos personales.

¿Qué deben hacer las empresas para estar en cumplimiento total con la nueva ley?

- Fomentar una cultura de protección de datos mediante la creación de un programa de privacidad y la confección de un modelo de prevención.
- Actualizar su matriz de riesgo, sus políticas y procedimientos relacionados con el tratamiento de datos personales, con foco en la determinación de riesgos y el establecimiento de medidas para mitigarlos, de manera que se adecuen a la realidad de la empresa. Los modelos de prevención son instrumentos vivos.
- **Mantenerse informadas sobre la nueva ley, como también de las normas específicas que pueda dictar la Agencia y la futura jurisprudencia administrativa.**

¿Necesitas asesoría?

El área de práctica de Tecnología, Ciberseguridad y Protección de Datos es liderada por Macarena Gatica y asesora a los clientes en materia de tratamiento de datos personales, comercio electrónico, ciberseguridad, adquisiciones, propiedad intelectual, licencias, transferencia de tecnología, outsourcing, software, hardware, joint ventures y alianzas estratégicas, en un amplio espectro de industrias y tecnologías.

Nos puedes contactar en:

https://alessandri.legal/contacto/

ALESSANDRI 130 AÑOS
ABOGADOS 1893