ManageEngine
Log360

Protección de datos personales en Chile

¿Su organización está cumpliendo con las leyes de privacidad chilenas?

www.manageengine.com/log360

Introducción

La Ley 19628, sobre Protección de la Vida Privada es una ley chilena que está en vigor desde 1999 y se ha actualizado periódicamente para adaptarse a los tiempos cambiantes. La última actualización se realizó el 26 de agosto de 2020. Sin embargo, la esencia de la ley sigue siendo la misma desde el momento de su institución. Los datos de carácter personal no deben ser comprometidos por ninguna entidad, privada o gubernamental. La entidad que ha almacenado los datos es totalmente responsable de su protección y uso dentro de los límites definidos por esta ley.

> “
> Artículo 2°.- Para los efectos de esta ley se entenderá por:
> n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal. ”

En este e-book hemos explorado algunos de los aspectos importantes de la ley y lo que significa para los administradores de seguridad. Incluso si no está bajo el ámbito de la ley, algunas de las medidas de protección de datos sugeridas aquí, pueden ayudarle a mejorar su postura de seguridad.

Responsabilidad de la organización

Esta ley brinda pautas claras sobre cómo se deben procesar y almacenar los datos personales. La organización debe formular pautas claras para garantizar que los datos solo se utilicen para el propósito establecido y que no se viole la privacidad de los usuarios de ninguna manera.

El rol del administrador de seguridad es crucial para garantizar que los datos se almacenen de manera segura y para cumplir con las solicitudes para eliminar o modificar los datos existentes.

1 Almacenar datos confidenciales del usuario de forma segura.

Según la ley, la responsabilidad de la organización es garantizar que los datos se almacenen de manera segura. Esto implica que debe haber suficientes controles de seguridad para que los ciberdelincuentes no tengan acceso a datos confidenciales de los usuarios. Por eso, es importante tener políticas de seguridad claramente definidas para evitar el robo de datos.

Para obtener más información sobre las medidas sencillas que puede adoptar para proteger su empresa, haga clic aquí.

> “Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.”

2 Cumplir con las solicitudes de modificación y eliminación de datos.

La organización que almacena los datos debe cumplir con las solicitudes de los usuarios para eliminar o modificar sus datos, si se realiza una solicitud por escrito. Para ello, es importante saber dónde se almacenan estos datos o si existen copias de ellos en algún lugar. Si existe alguna copia de los datos dentro de su organización después de que se haya cumplido con la solicitud, inadvertidamente estaría infringiendo la ley.

> “Artículo 2°.- Para los efectos de esta ley se entenderá por:
>
> h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.
>
> j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.”

3 Asegúrese de que solo las personas adecuadas tengan acceso a datos confidenciales.

Para acceder a datos sensibles, siga el principio de privilegio mínimo. Otorgue solo los permisos mínimos requeridos para los usuarios que manejan estos datos. Las solicitudes adicionales se pueden otorgar caso por caso. Una vez que un usuario no necesite acceder a esta información, asegúrese de revocar su acceso de inmediato.

> Artículo 7°.- Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

4 Siga de cerca la validez de los datos y las entidades con las que se han compartido, si corresponde.

Según esta ley, cualquier usuario tiene derecho a saber si sus datos han sido compartidos con alguna otra entidad. Si solicita esta información, están obligados a proporcionarla. También pueden solicitar que se modifiquen los datos si se encuentran inexactos. Además, si los datos están desactualizados o carecen de base legal para su almacenamiento, pueden solicitar su eliminación.

Para los administradores de seguridad, es importante verificar si los datos se han compartido y si su almacenamiento de datos es válido. Si ya no tiene la necesidad de almacenarlo, es mejor eliminarlo lo antes posible para evitar cualquier responsabilidad por el mismo.

> Título II: De los derechos de los titulares de datos
>
> Artículo 12.- Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.
>
> Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

ManageEngine
Log360

Cómo Log360 puede ayudar a cumplir con las leyes de protección de datos

Log360, la solución integral de administración de eventos e información de seguridad puede ayudarle superar los desafíos de cumplir con las leyes de privacidad incluso de GDPR, LGPD, NIST, CCPA y mucho mas.

Los módulos de Log360 ayudan a:

- Descubrir todas las instancias de datos sensibles dentro de su organización.
- Realizar un seguimiento de las modificaciones a los permisos de seguridad.
- Supervisar la integridad de los archivos.
- Detectar indicadores de una infracción con machine learning y alertas en tiempo real.

Si cree que una solución de gestión de eventos e información de seguridad (SIEM) le ayudará, puede probar Log360. Además, puede programar una demostración gratuita en la que nuestros expertos en productos responderán a sus preguntas sobre la solución y demostrarán las ventajas de utilizar Log360 en su organización.

ManageEngine
Log360

Log360, la solución integral de administración de eventos e información de seguridad puede ayudarle superar los desafíos de gestión de logs y seguridad de red. La solución recoge todos los logs de su red para dar información crítica en forma de informes, gráficos, y alertas. Con una herramienta tan versátil como esta, obtendrá un control completo sobre su red; podrá auditar cambios de Active Directory, los registros de dispositivos de red, los servidores de Microsoft Exchange, Microsoft Exchange Online, Azure Active Directory y su infraestructura de nube pública, todo desde una sola consola.

Para más información visite https://www.manageengine.com/latam/log-management/

$ Cotización ⬇ Descargar