EL MERCURIO Legal

Versión para imprimir El Mercurio.com

Menos datos, menos riesgo

"...La implementación de políticas de proporcionalidad en el tratamiento de datos, la eliminación de información innecesaria y la adopción de prácticas de privacidad desde el diseño no solo permitirán evitar sanciones regulatorias, sino que reducirán objetivamente la exposición a ciberataques, mejorarán la eficiencia operacional al gestionar menos datos, fortalecerán la confianza de clientes y socios comerciales, y facilitarán el cumplimiento de estándares internacionales que habilitan la transferencia transfronteriza de datos..."

Lunes, 9 de febrero de 2026 a las 19:45

Josefina Navarrete y José Minoletti

La entrada en vigencia de la Ley N° 21.719 ha obligado a las organizaciones a adaptar sus procesos de tratamiento de datos personales. Sin embargo, más allá del cumplimiento normativo existe un argumento adicional para que las organizaciones adopten prácticas más rigurosas en el manejo de datos: a mayor volumen de datos almacenados, mayor exposición a ciberataques.

La Ley N° 21.719 incorpora expresamente el principio de proporcionalidad, estableciendo que los datos tratados deben ser necesarios para los fines del tratamiento y conservarse solo el tiempo necesario para dicho cumplimiento. Esta obligación legal responde a una lógica de protección que, analizada en conjunto con la Ley N° 21.663, Ley Marco de Ciberseguridad, revela una lógica regulatoria coherente: reducir la superficie de exposición a amenazas digitales.

Los informes de ciberseguridad más recientes confirman una correlación directa entre el volumen de datos almacenados y la probabilidad de sufrir incidentes de seguridad. Según el *Q1 2025 Global Cyber Attack Report*, de Check Point Research, durante el primer trimestre de 2025 el promedio de ciberataques por organización semanal se incrementó un 47 % respecto al mismo período del año anterior, alcanzando 1.925 ataques por semana, y los incidentes de ransomware aumentaron un 126 % en ese mismo lapso. Este incremento está directamente vinculado a la adopción de servicios en la nube, el trabajo remoto y, fundamentalmente, a la acumulación indiscriminada de datos.

En ese contexto, se vuelve relevante el concepto "superficie de ataque", definido por el IBM como la suma de vulnerabilidades, caminos o métodos que los hackers pueden usar para obtener acceso no autorizado a la red o a datos sensibles.

La práctica de minimización de datos genera beneficios tangibles en materia de ciberseguridad. Al reducir el volumen y la variedad de datos almacenados, una organización disminuye su superficie de ataque. En caso de una brecha, el impacto potencial se contiene naturalmente, ya que los datos comprometidos son, por diseño, limitados.

Esta lógica se resume en un principio simple pero poderoso: los hackers no pueden robar lo que no existe. Las organizaciones que implementan políticas robustas de minimización de datos no solo cumplen con sus obligaciones legales bajo la Ley N° 21.719, sino que simultáneamente reducen su exposición a las consecuencias, financieras, reputacionales y regulatorias, de un eventual incidente de seguridad.

Como ya es de público conocimiento, la promulgación de las leyes N° 21.663 y N° 21.719 traen aparejadas sanciones significativas. Sin embargo, el costo regulatorio palidece frente al impacto económico de un ciberataque. Según el informe *Cost of a Data Breach 2025*, del IBM, el costo promedio global de una brecha de datos alcanzó los US$ 4.44 millones, mientras que en Estados Unidos superó los US$ 10 millones. El sector salud, por decimocuarto año consecutivo registró los costos más elevados, con un promedio de US$ 7.42 millones por incidente.

La adaptación a la Ley N° 21.719 no debe concebirse únicamente como un ejercicio de cumplimiento normativo. Las empresas que comprendan la relación intrínseca entre minimización de datos y ciberseguridad podrán transformar esta obligación legal en una ventaja competitiva.

La implementación de políticas de proporcionalidad en el tratamiento de datos, la eliminación de información innecesaria y la adopción de prácticas de privacidad desde el diseño no solo permitirán evitar sanciones regulatorias, sino que reducirán objetivamente la exposición a ciberataques, mejorarán la eficiencia operacional al gestionar menos datos, fortalecerán la confianza de clientes y socios comerciales, y facilitarán el cumplimiento de estándares internacionales que habilitan la transferencia transfronteriza de datos.

** Josefina Navarrete Bada y José Minoletti Ríos son asociados del equipo de Datos de Prieto.*

0 Comentarios Maria Concha ▼

M Sé el primero en comentar...

♡ **Comparte** **Mejores** **Más recientes** **Más antiguos**

Sé el primero en comentar.