DIARIO FINANCIERO®

Fecha: 12/05/2026 Audiencia: 40.297 Sección: ESPECIALES
Vpe: $2.160.799 Tirada: 13.432 Frecuencia: DIARIO
Vpe pág: $5.442.800 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 39,7%

LA HERENCIA DE DATOS QUE COMPLICA A LAS EMPRESAS ANTE LA NUEVA LEY

De cara a la entrada en vigencia de la nueva normativa en diciembre próximo, las organizaciones enfrentan el costo de ordenar bases de datos históricas construidas sin gobernanza clara, con riesgos que van desde multas y litigios hasta problemas operacionales y reputacionales. POR ANAÍS PERSSON

Durante años, las empresas chilenas acumularon información de clientes, trabajadores y proveedores bajo una lógica que pronto quedará obsoleta. Correos electrónicos obtenidos desde formularios web, bases comerciales construidas a partir de campañas antiguas, planillas compartidas entre áreas y datos almacenados indefinidamente pasaron a formar parte de un ecosistema que, con la entrada en vigencia de la nueva Ley de Protección de Datos Personales el próximo 1 de diciembre, se verá puesto a prueba.

El CEO de Jumpdot, Mauricio Palma, sostiene que parte importante del problema sigue estando en los puntos de entrada más básicos. "En algunos casos, los formularios y los pop-ups de 'suscríbete a nuestro newsletter' piden nombre, correo y teléfono sin explicar con claridad para qué se van a usar esos datos, sin un *checkbox* de aceptación expresa o sin un link visible a la política de privacidad", advierte.

No obstante, el gerente general de Fundación País Digital, Fernando Sánchez, afirma que el "talón de Aquiles del cumplimiento" es ordenar décadas de información acumulada. Según explica, muchas organizaciones avanzaron rápidamente en digitalización sin desarrollar una arquitectura clara de gestión de datos. El resultado fueron bases dispersas, duplicadas y administradas por distintas áreas sin trazabilidad completa sobre el origen, uso o eliminación de la información.

Según Víctor Saldaña, fundador de Kulvio y CEO de Solutoria, uno de los principales problemas que aparece en los diagnósticos es la falta de inventario. "Nadie en la organización tiene un mapa completo de qué tablas, qué archivos, qué buzones de correo

DIARIO FINANCIERO®

Fecha: 12/05/2026 Audiencia: 40.297 Sección: ESPECIALES
Vpe: $3.005.515 Tirada: 13.432 Frecuencia: DIARIO
Vpe pág: $8.127.680 Difusión: 13.432
Vpe portada: $21.104.600 Ocupación: 36,98%

y qué sistemas SaaS contienen datos personales", sostiene. Esto se traduce en planillas compartidas, bases de marketing antiguas y datos históricos guardados "por si acaso", además de información almacenada en sistemas que ya ni siquiera se utilizan.

A ello se suma el uso de datos obtenidos bajo consentimientos que la nueva normativa ya no admite, y la conservación indefinida de información. Según explica, muchas empresas siguen compartiendo datos con filiales o terceros sin suficiente respaldo y almacenando información durante años simplemente porque nunca se definieron plazos para eliminarla. El problema es que la nueva ley obligará a justificar cuánto tiempo se conservan esos datos y por qué.

"Las organizaciones asumían que si un dato estaba en internet o en un directorio, podían extraerlo y utilizarlo libremente. La nueva ley elimina esto como base de la licitud", explica el fundador y director de LegalDatos, Daniel Manríquez.

"A menos de siete meses de la entrada en vigencia, la ventana para la adecuación es estrecha. Auditorías de datos, definición de responsables, capacitación de equipos y actualización de políticas son trabajos que toman meses, no semanas, y que en muchos casos exigen reasignación de recursos relevantes", afirma Daniel Manríquez, de LegalDatos.

El riesgo de no actualizarse

De acuerdo con lo que establece la nueva normativa, las organizaciones cuentan con un período de transición de 24 meses desde su publicación para ajustar sus bases de datos existentes a la nueva ley.

La norma establece multas de hasta 5.000 UTM para infracciones leves, 10.000 UTM para graves y 20.000 UTM para gravísimas. "El golpe es mayor para la gran empresa: en caso de reincidencia, la sanción puede escalar hasta el 4% de sus ingresos anuales por ventas", añade Manríquez. A ello se suma el riesgo de litigios e indemnizaciones civiles, ya que también establece un régimen de responsabilidad civil frente a eventuales usos indebidos de datos personales.

Pero los expertos advierten que el impacto puede ir mucho más allá de las sanciones. "Una mala gestión de datos puede afectar la continuidad de servicios, la relación con clientes, la confianza de los usuarios y la capacidad de una empresa para trabajar con proveedores, aliados o mercados que ya exigen estándares más altos de privacidad y seguridad", afirma Sánchez.

La falta de gobernanza también incrementa la exposición frente a filtraciones y brechas de seguridad. Según el informe Cost of a Data Breach 2025 de IBM y Ponemon Institute, el costo promedio global de una brecha de datos alcanzó los US$ 4,44 millones entre marzo de 2025 y febrero de 2025, mientras en América Latina llegó a US$ 3,81 millones.

El especialista en ciberseguridad del Grupo Tecnológico ITQ, Jaime Marchant, explica que cumplir implica conformar equipos interdisciplinarios entre áreas legales, tecnológicas y de procesos, además de designar un delegado de protección de datos. También requiere un proceso de limpieza y gobernanza "que puede extenderse entre seis y 18 meses, dependiendo del volumen de información".

"A menos de siete meses de la entrada en vigencia, la ventana para la adecuación es estrecha. Auditorías de datos, definición de responsables, capacitación de equipos y actualización de políticas son trabajos que toman meses, no semanas, y que en muchos casos exigen reasignación de recursos relevantes", concluye Manríquez.