



Las empresas están incorporando nuevas capas tecnológicas para responder a una exigencia clave: saber qué datos personales tienen, dónde están, quién accede a ellos y cómo demostrar su correcto tratamiento, cuando faltan pocos meses para la entrada en vigencia de la Ley 21.719 sobre protección de datos personales.

"El principio de responsabilidad proactiva cambia completamente el escenario. Ya no basta con hacer las cosas bien, las organizaciones deben poder demostrarlo", explica el fundador y director de LegalDatos, Daniel Manríquez. En ese contexto, afirma que las herramientas de descubrimiento y mapeo permiten identificar información dispersa en bases de datos, correos, planillas o servicios cloud.

PROTECCIÓN DE DATOS PERSONALES

LAS TECNOLOGÍAS Y TENDENCIAS QUE ESTÁN AL SERVICIO DE LA PROTECCIÓN DE DATOS

Resolver problemas de visibilidad, trazabilidad y control de datos son algunos de los desafíos en que herramientas como la automatización están tomando fuerza. POR ANAÍL PERSSON

El CEO de Jumpdot, Mauricio Palma, explica que otra capa relevante es la clasificación de datos, que permite distinguir información sensible, como datos biométricos, financieros o de salud, para aplicar resguardo. También se suman tecnologías de trazabilidad, capaces de reconstruir el recorrido de un dato y acreditar bajo qué consentimiento fue obtenido.

La automatización también gana espacio. Según Palma, estas herramientas permiten gestionar solicitudes de acceso, rectificación o eliminación de datos dentro de los plazos que exige la ley. Para Manríquez, ayudan a enfrentar la práctica de acumular información "por si acaso", alertando para eliminar o anonimizar datos antiguos.

Otras necesidad creciente es

acreditar cumplimiento. El CIO de Kulvio, Alexis Cona, explica que las empresas requieren generar evidencia auditable para demostrar qué datos se trataron y bajo qué autorización. Agrega que las herramientas de control de accesos e identidades permiten limitar permisos y reducir riesgos de exposición.

Desde Entelgy Chile, su gerente de negocios de ciberseguridad, Pablo Álvarez, advierte que muchas empresas operan con baja visibilidad sobre datos y permisos excesivos, y que herramientas de monitoreo ayudan a detectar configuraciones inseguras.

A estas capas se suman herramientas de autenticación e identidad digital. El gerente general de Ecert, Alfredo Guardiola, sostiene que si una empresa no puede verificar la identidad de quien ejerce sus derechos sobre datos personales, "el proceso completo se vuelve vulnerable".

El nivel de preparación para implementar estas tecnologías sigue siendo desigual, advierten los expertos. Según Palma y Álvarez, sectores como banca, telecomunicaciones, retail y minería avanzan más rápido por exigencias regulatorias y estándares internacionales.