LITORALPRESS

Fecha: 29-04-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Columnas de Opinión
Título: COLUMNAS DE OPINIÓN: Seguridad no es privacidad

Pág. : 31
Cm2: 193,7

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

MARCELO DRAGO AGUIRRE
ABOGADO, SOCIO DATACOMPLIANCE, PRESIDENTE AGPD

Seguridad no es privacidad

En algunas empresas se sigue repitiendo una idea que conviene corregir cuanto antes: "Tenemos ISO 27001, por lo tanto estamos cumpliendo con la Ley de Protección de Datos Personales". La afirmación es equivocada. Y, en el nuevo escenario regulatorio, puede resultar costosa.

ISO 27001 es un marco serio y valioso. Permite ordenar la seguridad de la información, gestionar riesgos, establecer controles y fortalecer la capacidad de respuesta frente a incidentes. Pero su pregunta central es técnica: cómo proteger la información.

La Ley N° 21.719 plantea otra pregunta, de naturaleza jurídica y regulatoria: con qué fundamento se tratan datos personales, para qué fines, por cuánto tiempo y con qué resguardos respecto de los derechos de las personas.

Confundir ambos planos es un error de base.

Una organización puede estar muy bien preparada en seguridad y, al mismo tiempo, incumplir de manera grave en privacidad. Puede tratar datos sin base de licitud suficiente. Puede informar deficientemente a los titulares. Puede usar datos para finalidades distintas de aquellas que justificaron su recolección. Puede conservarlos más allá de lo necesario. Puede carecer de mecanismos eficaces para atender derechos. Puede transferirlos al extranjero sin garantías adecuadas. Puede, incluso, omitir evaluaciones de impacto en tratamientos de alto riesgo. Nada de eso queda resuelto por una certificación de seguridad.

> "El punto no es menor para los directorios ni la alta administración. El principal riesgo es la falsa sensación de cumplimiento".

Dicho de manera simple: una empresa puede tener una bóveda impecable y aun así estar infringiendo la ley respecto de aquello que guarda dentro. Porque la privacidad no se agota en proteger datos contra accesos indebidos. Exige, además, justificar su tratamiento, limitarlo, gobernarlo y hacerlo compatible con un derecho fundamental.

Este punto no es menor para los directorios ni para la alta administración. El principal riesgo no es solo una brecha de seguridad. También lo es la falsa sensación de cumplimiento. Creer que la ciberseguridad absorbe por completo la protección de datos puede llevar a decisiones erradas, brechas regulatorias invisibles, exposición sancionatoria y daño reputacional relevante.

En adelante, la conversación empresarial madura no debiera ser seguridad o privacidad. Debiera ser cómo integrar ambas en una misma arquitectura de cumplimiento. Seguridad de la información, sí. Pero también gobernanza de datos, políticas de retención, revisión de bases de licitud, gestión de derechos, evaluación de impactos y accountability real.

La seguridad protege sistemas. La privacidad protege personas.

Lo primero es indispensable. Lo segundo es un derecho fundamental. Y en el nuevo marco legal, entender esa diferencia ya no es una sofisticación doctrinaria. Es una necesidad de negocio.

Si una compañía cree que con ISO 27001 ya resolvió privacidad, probablemente no tiene resuelto el cumplimiento: apenas tiene resuelta una parte del problema.