LITORALPRESS

Fecha: 28-01-2026
Medio: Diario Financiero
Supl. : Diario Financiero - Inserto
Tipo: Noticia general
Título: ESLABÓN HUMANO: EL GRAN DESAFÍO DE LA SEGURIDAD DIGITAL

Pág. : 10
Cm2: 323,4

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

ESLABÓN HUMANO: EL GRAN DESAFÍO DE LA SEGURIDAD DIGITAL

Con nuevas exigencias legales en puerta, invertir en tecnología no basta si las empresas no cierran las brechas de capacidades y cultura en sus equipos.

POR ANAÍS PERSSON

Apesar de las inversiones en tecnología y sistemas de seguridad, una parte importante de los incidentes y filtraciones de datos sigue teniendo un origen mucho más básico: errores humanos, malas prácticas o decisiones tomadas bajo presión. En un escenario donde la nueva Ley de Protección de Datos eleva el estándar de responsabilidad, el foco empieza a desplazarse desde la infraestructura hacia las personas.

"Cerca del 97% de los incidentes de ciberseguridad tiene su origen en factores humanos", señala el socio de consulting y líder en ciberseguridad de KPMG Chile, Erick Palencia. Al hacer su análisis sobre la realidad local, agrega que "solo durante el primer trimestre de 2025 se registraron más de 15 millones de intentos de ciberataques, con un aumento cercano al 32% respecto del año anterior", y advierte que "las organizaciones reciben, en promedio, 2.037 ataques por semana".

Para el fundador y CEO de Prey, Carlos Yaconi, el diagnóstico es claro: "El factor humano sigue siendo el punto más débil y, al mismo tiempo, la primera línea de defensa". Plantea que la mayoría de los incidentes graves "no nace de una falla técnica, sino de un descuido o una mala práctica". Pero ese mismo factor también puede marcar la diferencia: "Una persona que sabe reconocer una señal de riesgo puede evitar que un error escale a una crisis mayor".

En este escenario, Palencia advierte que hoy se necesitan perfiles híbridos: "Profesionales de tecnología que comprendan el marco normativo, o abogados que entiendan los sistemas y riesgos tecnológicos". Y, desde el lado de los dueños de proceso, indica que "existe una brecha relevante de conocimiento sobre cómo los principios de protección de datos impactan sus operaciones".

"La principal brecha no es técnica, sino cultural. La alta gerencia aún no lidera estos procesos como prioridad estratégica, y sin ese impulso no hay presupuesto ni continuidad", afirma Yaconi. Además, advierte que "lo transversal no se logra con una charla masiva, sino que conectando lo tecnológico, lo legal y la operación diaria".

La nueva ley viene a endurecer ese estándar. Según el CLO de LeyDeDatos, Ignacio Gallardo, "el foco de la organización debe ser tanto transversal como focalizado: toda la organización debe comprender los principios básicos, pero las áreas que participan directamente en el tratamiento de datos deben asumir responsabilidades específicas y acorde a los riesgos que gestionan".

En ese marco, hay prácticas habituales hasta que dejan de ser aceptables. "La normativa busca que cada persona sepa cuál es su rol y cómo debe interactuar con los datos personales. Mantener información personal indefinidamente 'por si acaso' no será tolerado bajo el nuevo marco regulatorio", concluye.