LITORALPRESS

Fecha: 27-01-2026
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: ¿Las empresas chilenas invierten en ciberseguridad?

Pág. : 23
Cm2: 430,8

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

Más de la mitad no cuenta con un calendario regular de evaluaciones de riesgo

¿Las empresas chilenas invierten en ciberseguridad?

Según estudios recientes, las amenazas tienen una respuesta reactiva en nuestro país.

Pareciera ser que en Chile la ciberseguridad aún no es un tema prioritario. Según una reciente encuesta de la consultora Kaspersky, más de la mitad de las organizaciones (56%) no cuenta con un calendario regular de evaluaciones de riesgo.

Esto confirma que, ante este tipo de escenarios, las empresas chilenas siguen siendo reactivas más que proactivas, actuando en respuesta a las contingencias en lugar de anticiparse a los ataques cibernéticos o los cambios del entorno digital.

El estudio también revela que, aunque la mayoría de las empresas realiza simulaciones de incidentes, 76% no tiene ninguna rutina de pruebas.

Otro dato relevante es que 38% de los encuestados afirma no contar con una estrategia clara de seguridad. Esto refuerza que, para muchas organizaciones, el desafío no sólo está en saber qué se necesita hacer, sino en la falta de una directriz estructurada que guíe las decisiones, priorice los recursos y defina el nivel mínimo de protección necesario.

Esta falta de disciplina para identificar y revisar debilidades y riesgos deriva en otro problema identificado por los expertos: una disparidad entre la confianza que las empresas tienen en su protección digital y el nivel de seguridad que poseen en realidad.

CEDIDA

Expertos subrayan que a todo nivel corporativo es necesario tener una estrategia de ciberseguridad.

"Cuando una organización no cuenta con una lectura precisa de su situación en ciberseguridad, las decisiones sobre dónde y cómo invertir se vuelven imprecisas y difíciles de justificar. La falta de métricas sólidas termina convirtiendo el ROI (retorno sobre inversión) en un cálculo incierto", advierte Andrea Fernández, gerente general para la Región Sur de América Latina en Kaspersky.

"En cambio, cuando la empresa comprende claramente su nivel actual de madurez y el punto al que desea llegar, es posible estructurar un plan de inversión progresivo, con objetivos concretos y resultados esperados, lo que facilita tanto la gestión operativa como la evaluación del retorno", agrega.

Mejor inteligencia

Por otro lado, la omnipresente inteligencia artificial está ayudando a que todos estos procesos pasen a ser un poco más orgánicos y adaptables para las empresas, dependiendo del tamaño y la necesidad, claro está.

Según un estudio local realizado por Microsoft Chile, 52% de las empresas cuentan con políticas formales para el uso de agentes de IA y ocho de cada diez consideran que estos lineamientos son efectivos. Aunque la percepción de efectividad varía según el tipo de organización, en empresas nativas digitales 40% califica estas políticas como altamente efectivas, mientras que en las no nativas digitales este nivel alcanza sólo 27%.

En términos de ciberseguridad, actualmente 61% de las organizaciones ya emplea agentes de IA en sus procesos de ciberseguridad, mientras que 35% está considerando su incorporación, lo que demuestra una tendencia sostenida hacia su adopción.

El uso de estas tecnologías se extiende transversalmente a múltiples áreas funcionales, destacando experimentos en servicios críticos como atención al cliente (57%), infraestructura tecnológica (57%), finanzas (50%) y ventas/marketing (50%). Para Marcelo Felman, director de Ciberseguridad de Microsoft para América Latina, "la IA no solo aumenta la velocidad y el alcance de las defensas: a través de agentes especializados, ayuda a cerrar brechas de talento, estandarizar procesos y elevar la resiliencia del negocio. El desafío ya no es si invertir en seguridad, sino cómo escalarla con IA y gobernanza responsable en cada capa de la organización".