Chile frente al avance de los ciberataques: más preparado, pero también más expuesto

• *La alta digitalización del país lo posiciona como un blanco prioritario en la región, en un escenario donde las amenazas son cada vez más precisas y sofisticadas.*

Si bien los mecanismos de defensa del país en materia de ciberseguridad han evolucionado más respecto a la región latinoamericana, la alta digitalización incrementa su vulnerabilidad, sostuvo el académico de la Escuela de Ingeniería Informática de la Pontificia Universidad Católica de Valparaíso, Sebastián Berríos.

La ciberseguridad se ha convertido en una práctica imprescindible a nivel global, dado el aumento de los riesgos digitales que afectan tanto a instituciones públicas como privadas. Chile enfrenta un escenario cada vez más desafiante en esta materia, pues según cifras del 2026, el país continúa siendo uno los principales objetivos de ciberataques en la región, registrando un promedio de 1.700 intentos semanales por organización.

Según explicó el académico de la casa de estudio, la transformación más relevante que han experimentado las amenazas digitales no solo está en el volumen, sino en sus niveles de precisión y efectividad. “Ya no vemos tantos ataques masivos al azar; ahora vemos operaciones quirúrgicas dirigidas al corazón de nuestra infraestructura crítica, como servicios de salud, banca y energía”, precisó.

Ley Marco

Uno de los hitos recientes a nivel nacional fue la promulgación de la Ley Marco de Ciberseguridad (Ley 21.663),

el año 2024, donde se estableció un nuevo sistema regulatorio para la gestión de riesgos digitales en el país. La normativa creó la Agencia Nacional de Ciberseguridad (ANCI), que tiene como misión fortalecer la ciberseguridad nacional para reducir las amenazas digitales, aumentar la protección de los servicios esenciales y resguardar los derechos de las personas en el entorno digital.

Al respecto, el académico señaló que el aporte de esta normativa es histórico, pues la seguridad pasó de ser un tema técnico a una responsabilidad legal. “Las multas ahora son significativas y la obligación de reportar incidentes está forzando una cultura de transparencia. La normativa ha impulsado la gobernanza de la ciberseguridad a nivel estratégico, obligando a las organizaciones a incorporar gestión de riesgos y reportabilidad”, agregó.

Pese a esta preparación, el especialista advirtió que vivimos en una situación ambivalente, pues si bien Chile ha avanzado más que cualquier otro país de la región en el marco institucional, nuestra alta digitalización nos hace más vulnerables: “somos el ‘alumno más aventajado’ de Latinoamérica, pero eso mismo nos pone una diana en la espalda”.

Errores más comunes e impacto de la IA

El académico de la PUCV explicó que los errores más frecuentes en materia de ciberseguridad son al menos tres: carencia de Autenticación Multi-Factor (MFA); sistemas desactualizados por no instalar parches oportunamente y descuido del factor humano, donde hace falta entrenar a los empleados para la detección de engaños por Inteligencia Artificial.

A propósito de esta última, indicó que se trata de un acelerador de doble filo: “Para los atacantes, la IA ha democratizado el cibercrimen permitiendo crear Deepfakes de voz para suplantar identidades. Para la defensa, en tanto, es

nuestra mejor aliada, pues es la única herramienta capaz de procesar millones de eventos por segundo, para detectar anomalías antes de que el daño sea irreversible", puntualizó.

PUCV y entorno digital

En el marco de estos grandes desafíos, cabe destacar que la PUCV, a través de la Escuela de Ingeniería Informática, no solo forma profesionales altamente capacitados para desempeñarse en ámbitos como la ciberseguridad y la transformación digital, sino que dentro de su Plan de Desarrollo Estratégico, también declara como uno de sus principales objetivos "fortalecer la cultura institucional para la transformación digital", buscando así robustecer las competencias de su comunidad académica y promover la ética y la ciudadanía digital.