FRENTE A SU RÁPIDA EVOLUCIÓN:

Ciberinteligencia y ciberresiliencia, fundamentales ante las amenazas

La combinación de nuevas tecnologías, la presión regulatoria y las tensiones geopolíticas complican la gestión de los riesgos a nivel mundial.

CATERINNA GIOVANNINI

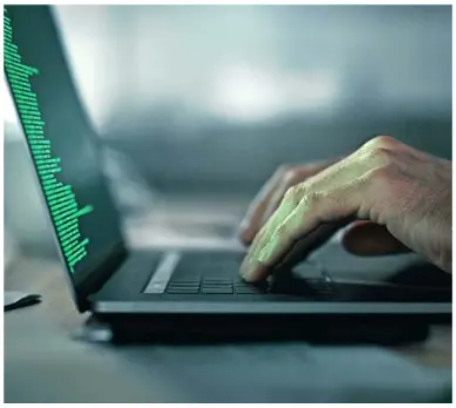
La complejidad y la impredictibilidad del panorama cibernético están aumentando, dice el Global Cybersecurity Outlook 2025, del Foro Económico Mundial. Esto, porque al mismo tiempo que se multiplican los requisitos normativos para las empresas en materia de ciberseguridad, el escenario está cada vez más cargado de tensiones geopolíticas, hay una mayor dependencia de cadenas de suministro complejas y se acelera la adopción de tecnologías emergentes, lo que hace "extremadamente difícil gestionar eficazmente los riesgos", señala el informe.

Los resultados de este año muestran también que los métodos de ataque conocidos, como el *ransomware* y el compromiso del correo electrónico empresarial (BEC), están aumentando su eficacia y alcance, mientras que el costo de las campañas de *phishing* o ingeniería social está disminuyendo gracias a tecnologías como la inteligencia artificial generativa.

Ignacio Hidalgo, gerente comercial de Banca y Minería de Claro Empresas, explica que los sectores más afectados son los servicios financieros, de salud, energía y servicios públicos. "Hoy, las infraestructuras críticas son un blanco por su impacto potencial y vulnerabilidades en tecnología operacional", dice, además del *retail* y comercio electrónico. Sin embargo, el ejecutivo agrega que para anticipar y prepararse ante posibles ataques existen soluciones enfocadas en lo que se conoce como ciberinteligencia y ciberresiliencia, que permiten a las organizaciones recuperarse y mantener la continuidad de sus operaciones.

Algunas de las acciones de prevención que Claro Empresas recomienda a sus clientes son el uso de soluciones de Mobile Device Management (MDM Cloud) para mitigar riesgos en la red e infraestructura TI y proteger las redes y datos corporativos en dispositivos de usuarios remotos, como *tablets*, *smartphones* y *laptops*; informes técnicos y ejecutivos con recomendaciones para analizar la vulnerabilidad en la nube de las empresas, e incluso un "hacking ético", en el que se penetra en el servicio de un cliente o dispositivo para comprobar la robustez de los controles de seguridad implementados en la organización.

Y aunque en el informe del Foro Económico Mundial se señala que el 42% de los encuestados en América Latina desconfía de la capacidad de su país para responder a incidentes cibernéticos graves contra infraestructuras críticas, Hidalgo ha observado que en Chile, si bien hay una alta tasa de ataques, se ha invertido en esta área consistentemente. "De hecho, de acuerdo con el Índice Nacional de Ciberseguridad, que mide la preparación de las naciones para prevenir amenazas cibernéticas y gestionar incidentes, en 2020 nos ubicábamos en el puesto 56 y ya en 2024 habíamos alcanzado el puesto 25", señala.



LAS DIVERSAS HERRAMIENTAS maliciosas están aumentando en frecuencia y reduciendo sus costos.