DIARIO FINANCIERO®

Fecha: 06/02/2025 Audiencia: 48.450 Sección: ECONOMIA
Vpe: $1.763.454 Tirada: 16.150 Frecuencia: DIARIO
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 23,69%

LA COLUMNA DE...

CARLOS CRUZ INFANTE
COUNTRY MANAGER
CEFEIDAS GROUP CHILE & PERÚ

La guerra invisible de Sudamérica: sabotaje digital

Cada inicio de año es usual la publicación de diagnósticos de riesgos geopolíticos más alarmantes y es en esa línea que Southcom, la división del Departamento de Defensa de Estados Unidos para el Caribe y Sudamérica dio también su opinión. A fines de 2024, la saliente General Laura Richardson identificó el ciberataque como uno de los principales riesgos para Sudamérica.

Aunque no se le dio tanta importancia a este riesgo en los informes de 2025, la amenaza es clara: a noviembre de 2024, América Latina había experimentado la tasa de crecimiento de ciberataques más rápida del mundo, con un alza promedio anual de 25% en la última década, según concluyó Estefania Vergara Cobos, investigadora del Banco Mundial.

Desde los '2020 ha ganado lugar la llamada Geopolítica del Malware, un despliegue masivo de ciberespionaje y ataques coordinados a gobiernos y la banca, generalmente respaldados por regímenes autoritarios, como Norcorea, que orquestó el famoso Grupo Lazarus; o el Gobierno chino, que apoyó al grupo de hackers autodenominados Salt Typhoon, poniendo en jaque a ocho proveedores de telecomunicaciones en EEUU.

En 2022 Costa Rica sufrió uno de los ataques más relevantes por parte del grupo Conti, declarado por el Gobierno como emergencia nacional y exigiendo US$ 20 millones para detener la ofensiva. Conti también se adjudicó el ataque a los servicios de inteligencia de Perú de ese año. Además, en 2023, un ataque a una empresa norteamericana afectó al Gobierno y la infraestructura de Colombia.

Chile no escapa a esta guerra invisible: solo en 2024 fuimos víctimas de 6,4 mil millones de intentos de ciberataques. El CEO de la aseguradora Marsh en Chile, afirmó a este medio que las pólizas de seguro para estos siniestros acumulan un aumento de más del 40% en octubre del año pasado y que además de la operación de los negocios o gobiernos afectados, los ciberataques podrían amenazar a los directores de empresas del país, dada la reciente Ley de Delitos Económicos.

> "Chile no escapa a esta guerra invisible: solo en 2024 fuimos víctimas de 6,4 mil millones de intentos de ciberataques".

Acá ha habido casos emblemáticos. Banco Santander fue atacado no solo en Chile, sino también en España y Uruguay. BancoEstado fue víctima de un millonario fraude interno. En 2023, un ciberataque masivo amenazó la continuidad operacional de Correos de Chile, Fonasa y el Servicio de Impuestos Internos, así como de 72 municipios.

El Gobierno ha tomado medidas. En 2023 publicó su Política Nacional de Ciberseguridad 2023-2028 y en marzo de 2024 promulgó La Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, que crea la Agencia Nacional de Ciberseguridad. Asimismo, el mes pasado Chile ingresó a la Counter Ransomware Initiative (CRI), lanzada en 2021 por Estados Unidos para coordinar políticamente los ataques maliciosos de robo de información.

Todas estas iniciativas parecen ir en la dirección correcta. Sin embargo, los esfuerzos regionales deben acentuarse. La CRI es un paso pero, como en todo sistema, las células abren paso a otras células. Chile, sobre todo, dado su masificado uso de plataformas de datos, y debido a su naturaleza de economía abierta al mundo, es un nodo más del Cono Sur, de la Alianza del Pacífico, de América Latina; ni Los Andes, ni el Pacífico ni el Desierto de Atacama serán suficientes para frenar el sabotaje digital, como tampoco lo serán las leyes circunscritas a nuestro territorio.