LITORALPRESS

Fecha: 23-06-2025
Medio: El Sur
Supl. : El Sur
Tipo: Noticia general
Título: **Prevención de los ciberataques**

Pág. : 2
Cm2: 280,4

Tiraje: 10.000
Lectoría: 30.000
Favorabilidad: No Definida

# Prevención de los ciberataques

Chile recibió 27.600 millones de intentos de ciberataques en 2024, frente a los 6.000 millones del año 2023, según datos dados a conocer hace unos días por FortiGuard Labs, el laboratorio de análisis e inteligencia de amenazas de Fortinet.

Los datos revelan que los actores de amenazas están utilizando de manera exponencial la automatización, las herramientas mercantilizadas e inteligencia artificial (IA) para erosionar de manera sistemática las ventajas antes sostenidas por los defensores. El reporte sobre el panorama global de amenazas de 2025 deja en claro que los cibercriminales están acelerando sus esfuerzos, utilizando IA y automatización para operar a niveles sin precedentes de rapidez y escala, dijo la empresa.

Ésta es una tendencia global ya que se observa una menor cantidad de ataques masivos y un mayor volumen de explotaciones únicas y variantes nuevas de malware y ransomware, que son mucho más dirigidos. Esto significa que hay menos cantidad de ataques pero son diseñados para objetivos específicos, lo que los vuelve más sofisticados y con mayor posibilidad de éxito si las organizaciones no cuentan con defensas de ciberseguridad actualizadas.

Pero el manual tradicional de seguridad ya no es suficiente. Las organizaciones deben tomar una estrategia proactiva enfocada en inteligencia e impulsada por IA, confianza cero y manejo continuo de exposición a amenazas, para poder mantenerse a la vanguardia del panorama de amenazas actual que está cada vez más evolucionado".

El cibercrimen impulsado por IA está escalando de manera rápida: los actores de amenazas están aprovechando la inteligencia artificial para mejorar el realismo del phishing y evadir los controles de seguridad tradicionales, lo que hace que los ciberataques sean más efectivos y difíciles de detectar. Herramientas para crear amenazas están impulsando campañas más escalables, creíbles y efectivas, sin las restricciones éticas de las herramientas de IA disponibles públicamente.

Se intensifican los ataques dirigidos a sectores críticos: industrias como manufactura, salud y servicios financieros continúan experimentando un aumento de ciberataques personalizados, con adversarios que despliegan exploits específicos para cada sector. En 2024, los sectores más atacados fueron manufactura (17%), servicios empresariales (11%), construcción (9%) y comercio minorista (9%).

A pesar de que las organizaciones de Chile están encaminadas hacia un proceso de transformación digital y fortalecimiento de la ciberseguridad, los resultados son insuficientes. Según el National Cyber Security Index, Chile se encuentra en el puesto 56 a nivel mundial, mientras que a nivel latinoamericano está en el cuarto lugar, por debajo de Paraguay, Argentina y Perú, lo que se traduce en una caída de diez puestos de la tabla.

**Según datos dados a conocer hace unos días por FortiGuard Labs, Chile recibió 27.600 millones de intentos de ciberataques en 2024, frente a los 6.000 millones del año 2023.**

Los especialistas dicen que el ataque más recurrente en Chile ha sido el ransomware, una técnica utilizada por los hackers para bloquear dispositivos, ya sea para demostrar su poder o para exigir un rescate a cambio de recuperar el acceso. Nuestro país se ubica en el tercer lugar en Latinoamérica y es décimo en el mundo entre los que más sufren ataques por ransomware. La segunda amenaza recurrente es el phishing o robo de información personal, como contraseñas o datos de tarjetas de crédito, que perjudica principalmente actividades y clientes del comercio mayorista, multitiendas y empresas de servicio. En tercer lugar, están los ataques web, donde Chile ocupa también el tercer lugar en Latinoamérica..

Los expertos indican que ha habido un aumento de este tipo de ataques selectivos a nivel mundial, provocados por bandas organizadas, con conocimientos sofisticados sobre vulnerabilidades, lo que obliga a tener una actitud proactiva en cuanto a la protección de datos para mitigar los riesgos.