LITORALPRESS

Fecha: 25-06-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Más de la mifad de las empresas en Chile pagaron rescatestras secuestro de datos en el primer trimestre

Pág. : 24
Cm2: 250,5

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

# Más de la mitad de las empresas en Chile pagaron rescates tras secuestro de datos en el primer trimestre

**Reporte de Sophos señaló que la causa principal de los ciberataques está en "vulnerabilidades conocidas no corregidas" y que pagar solo aumentará las amenazas.**

El informe *The State of Ransomware in Chile 2025* de Sophos, reveló que el 56% de las organizaciones chilenas afectadas por *ransomware* (secuestro de datos) durante el primer trimestre de 2025, pagó rescates por su información, con un monto promedio de US$ 675 mil.

El reporte se basó en encuestas realizadas entre enero y marzo a 122 empresas de diversos sectores -como finanzas y seguros, energía, gobierno local y central, manufactura y salud- con ingresos anuales de US$ 5 millones a US$ 50 mil millones. De ellas, la mitad tiene de 100 a 1.000 empleados, y la otra, entre 1.001 a 5 mil.

El gerente de ingeniería de Sophos para Latinoamérica, Rodolfo Castro, dijo que algunas firmas pagan para retomar operaciones rápidamente o evitar que trascienda el incidente, lo que aumentará la cantidad de amenazas.

"Más allá de recuperar su información, están propiciando las organizaciones criminales y atrayendo a más grupos organizados a ver a Chile como un mercado rentable y que paga. Por consiguiente, la cantidad y la agresividad de los ataques va a aumentar. La empresa pasa de ser víctima a victimario porque está patrocinando una organización criminal", afirmó.

Según el informe, el 46% de los ataques tuvo como causa raíz la explotación de vulnerabilidades, seguido por credenciales comprometidas (22%), correos maliciosos (20%), *phishing* -suplantación de identidad- (6%) y ataques de fuerza bruta (4%).

Castro explicó que cuando se habla de una vulnerabilidad explotada es "porque ya está documentada", se sabe cuál es el producto y posiblemente ya tenga un parche (actualización), pero no se continuó parchando. "Esto se puede deber al uso de sistemas operativos antiguos o la falta de un plan efectivo de parcheo", dijo.

**US$ 675 MIL**
ENTREGARON EN PROMEDIO POR RESCATE.

## Brechas de seguridad

El reporte identificó que el 55% de las empresas reconoció tener brechas de seguridad conocidas, seguido por falta de experticia (46%) y capacidad limitada o escasez de talento (44%).

Para Castro muchas compañías locales "no están preparadas" y siguen operando sin planes formales de respuesta a incidentes, y "cada vez es más normal que todo (plan y gestión de ciberseguridad) esté concentrado en una o dos personas", lo que eleva sus posibilidades de ser víctima de un ataque.

Comentó que existe una carencia de talento especializado en ciberseguridad, sobre todo en perfiles de CISO (sigla en inglés de director de seguridad de la información). El problema es que "desde el lado malo, las organizaciones criminales están reclutando gente para meterse en este mundo, que es muy bien pagado", afirmó.