DIARIO FINANCIERO®

Fecha: 02/04/2025 Audiencia: 48.450 Sección: PORTADA
Vpe: $6.368.689 Tirada: 16.150 Frecuencia: OTRAS
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 85,56%

DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
MIÉRCOLES 2 DE ABRIL DE 2025

CIBERSEGURIDAD

POR QUÉ RESPALDAR LA INFORMACIÓN ES CLAVE PARA PROTEGERSE DE LOS CIBERATACANTES

La filtración o pérdida de datos puede ser un grave problema para empresas y usuarios, un riesgo que aumenta ante ataques que buscan interrupir operaciones o robar información sensible y privada. Una cultura preventiva con foco en el backup es crucial para evitar estas situaciones.

POR MACARENA PACULL M.

La información y los datos son uno de los activos clave tanto para las compañías como para las personas, y su integridad está cada vez más comprometida al aumentar los ciberataques y sus modos de operar. Las cifras hablan por sí solas: un estudio de Kaspersky, que abarcó 19 países, reveló que el 75% de los encuestados calificó a las brechas de seguridad como "graves", tras causar la filtración de datos confidenciales o impactos negativos en la reputación de la compañía o en su situación financiera. En Chile, esta cifra llegó al 90% de los consultados.

Y es que los ataques siguen avanzando en número y complejidad. Otro informe de la misma empresa evidenció que entre octubre de 2023 y octubre de 2024 solo en Chile se bloquearon diariamente 38 mil ataques de phishing, técnica dedicada a fraudes bancarios y al robo de información. Durante ese año, además, se registraron 29 mil episodios de malware, con foco en el cifrado de datos para exigir un pago para su liberación.

Poner atención en las amenazas más comunes es necesario para poder identificar estos ataques. En este sentido, el gerente senior de ingeniería para Fortinet Chile, Juan Pablo Arias, alude a la importancia de los intentos de vulneraciones en el país: según FortiGuard Labs, Chile registró más de 27.600 millones de intentos de ciberataques en 2024, consolidándose como un foco activo para el cibercrimen.

"Dentro de las amenazas más comunes para las empresas sigue apareciendo el ransomware, muchas veces dirigido a las cadenas de suministro con la finalidad de generar un gran impacto y, por tanto, una mayor probabilidad de pagar el rescate", sostiene Arias, y apunta que en el caso de las personas, las amenazas más comunes tienen que ver con estafas por ingeniería social, robo de identidad y suplantación en redes sociales.

"En ambos casos, tanto para personas como empresas, el phishing potenciado por técnicas avanzadas de IA e ingeniería social se sigue posicionando como uno de los principales vectores de ataque", enfatiza el experto, quien hace hincapié en que las amenazas por fallas técnicas están asociadas a configuraciones incorrectas, sobre todo en entornos cloud y a sistemas legados con falta de parchado o actualizaciones que quedan expuestas.

Prevenir y proteger

Una de las acciones claves que menciona la directora de magíster en gestión de tecnología de la información y telecomunicaciones de la Facultad de Ingeniería de la Universidad Andrés Bello, Mailyn Calderón, es seguir la regla 3-2-1: "Tener tres copias de los datos, dos tipos de almacenamiento diferentes y una copia fuera del sitio, como en la nube", explica, en vista del Verizon Data Breach Investigations Report 2024, que reveló que el 36% de las brechas de datos se deben a contraseñas débiles, por lo que es importante cifrar y guardar las copias de seguridad en lugares seguros.

Además, Calderón señala que es recomendable mejorar las contraseñas utilizando combinaciones complejas o incluso usar un gestor de contraseñas para facilitar su gestión. "También es importante hacer respaldos diarios o semanales según la importancia de los datos y probar la restauración al menos una vez al año para asegurar que todo funcione bien", subraya.

Por su parte, Arias añade que para enfrentar eficazmente amenazas como el ransomware, es clave adoptar arquitecturas de ciberseguridad resilientes, que integren prevención, detección temprana y respuesta automatizada. "Esto implica implementar soluciones avanzadas con inteligencia artificial, especialmente para la protección en entornos cloud, capaces de identificar y bloquear comportamientos maliciosos en tiempo real", dice.

"Como medida de mitigación clave, el respaldo de información debe ser parte de toda estrategia de continuidad operativa y seguridad de datos", dice Carlo Seves San Martín, gerente comercial y marketing de SSeguridad, lo que tiene que ver no solo con la exposición a potenciales atacantes, sino también con fallas de hardware, actualizaciones mal ejecutadas, eliminación accidental de archivos o configuraciones inseguras. "Un backup bien gestionado puede reducir el tiempo de recuperación (RTO) de días a horas, con un impacto mínimo en la operación", recalca.

28 MIL
SON LOS EXPERTOS EN CIBERSEGURIDAD QUE NECESITA CHILE, SEGÚN CSIRT NACIONAL.

84%
DE LAS EMPRESAS EN CHILE CONSIDERA QUE LOS CIBERATAQUES CON IA SON UNA SERIA AMENAZA, SEGÚN KASPERSKY.