DIARIO FINANCIERO®

Fecha: 31/03/2026 Audiencia: 48.450 Sección: ciberseguridad y protección [illegible]s personal
Vpe: $5.505.765 Tirada: 16.150 Frecuencia: 0
Vpe pág: $7.443.240 Difusión: 16.150
Vpe portada: $7.443.240 Ocupación: 73,97%

EL BACKUP COMO EJE DE LA CIBERSEGURIDAD MODERNA

Expertos advierten que, ante el aumento de incidentes y fallas operativas, contar con estrategias de respaldo robustas dejó de ser una práctica técnica para convertirse en un pilar clave de la continuidad del negocio.

POR ANAÍS PERSSON

Cada 31 de marzo se conmemora el Día Mundial del *Backup*, una fecha que busca generar conciencia sobre la importancia de respaldar la información digital. En un contexto donde las empresas se enfrentan a la amenaza de los ciberataques, esta estrategia es una respuesta óptima y siempre recomendada por expertos para apoyar la continuidad operacional de las organizaciones.

Según el último informe de Check Point Research, América Latina es hoy la región más golpeada por ciberataques, con un promedio de 3.123 ataques semanales por organización durante febrero de este año y un crecimiento interanual de 20%. En el caso de Chile, se registraron, en promedio, 1.780 ataques, lo que representa una disminución de 4% respecto al mismo período del año anterior.

Al evaluar el desempeño de Chile en este escenario, la directora subrogante de la Agencia Nacional de Ciberseguridad (ANCI), Michelle Bordachar, dice que el país ha dado importantes pasos, particularmente con la implementación de la Ley Marco de Ciberseguridad y la creación de la agencia. No obstante, menciona que, si bien hay sectores que han madurado significativamente, otros todavía no incorporan la seguridad digital "como parte esencial de su operación ni tienen planes claros para mantener sus servicios funcionando si algo falla".

"Contar con una estrategia de respaldo de datos ya no es opcional: es indispensable. Sin ella, cualquier incidente que comprometa la información puede resultar catastrófico. Y no se trata solo de ataques informáticos, los errores humanos, accidentes, incendios o inundaciones también pueden borrar datos críticos de un momento a otro", afirma.

El costo de no protegerse

"La pérdida de acceso a la información genera costos en múltiples dimensiones, desde la reputación de los clientes hasta ventas no concretadas o derechamente pérdidas por no poder realizar la transacción", señala el gerente de desarrollo de negocios de Nubatech, Luis González. A esto se suman posibles multas regulatorias y gastos asociados a brechas de seguridad.

En la misma línea, el gerente de Servicios SyA, Ricardo Riquelme, advierte que la incapacidad de recuperación de información tras un ataque o algún evento de otra naturaleza puede afectar la reputación del negocio. "Cuando una empresa demuestra incapacidad para recuperarse con rapidez, el mayor impacto es la pérdida de confianza de sus clientes, quienes en el corto o mediano plazo buscarán alternativas confiables", señala.

HASTA US$ **1,23 MILLONES** PUEDE COSTAR UN INCIDENTE DE FUGA DE DATOS, SEGÚN CÁLCULOS DE KASPERSKY.

1.780 CIBERATAQUES SEMANALES POR ORGANIZACIÓN SE REGISTRARON DURANTE FEBRERO EN CHILE, SEGÚN CHECK POINT RESEARCH.

De acuerdo con datos de Kaspersky, el costo promedio de un incidente de fuga de datos alcanza los US$ 1,23 millones en grandes empresas y US$ 120 mil en pequeños negocios, lo que refuerza la necesidad de adoptar medidas proactivas de protección y recuperación de información.

El director del equipo global de investigación y análisis de esa firma para América Latina, Fabio Assolini, señala que el *ransomware* seguirá siendo una de las principales amenazas. "Las copias de seguridad son una regla esencial que debe ser parte del protocolo de ciberseguridad de todas las organizaciones, sin importar su tamaño o sector", indica.

Recomendaciones

Según Assolini, existe "una brecha importante" entre la percepción y la realidad. Citando datos de Kaspersky, indica que el 72% de las empresas en Chile considera tener una estrategia proactiva de ciberseguridad, pero en la práctica existen carencias importantes: más de la mitad opera sin *firewall*, un 30% no utiliza inteligencia de amenazas y un 32% no cuenta con antivirus.

A esto se suman errores comunes en la implementación de estrategias de respaldo. Riquelme identifica cinco prácticas frecuentes: ver el *backup* solo como un componente tecnológico y no como algo estratégico, no contar con planes de recuperación probados, mantener las copias en la misma red productiva, no disponer de copias aisladas e inmutables y la falta de capacitación del personal.

Para fortalecer la resiliencia digital, desde la Agencia Nacional de Ciberseguridad recomiendan adoptar la regla 3-2-1-1-0, considerada el estándar de oro del respaldo: mantener tres copias de los datos, en dos medios distintos, con una copia fuera de las instalaciones, una offline y cero errores verificados.

Además, los expertos recomiendan contar con sistemas de monitoreo, encriptación de datos, infraestructura redundante y almacenamiento distribuido entre entornos locales y en la nube. También es clave realizar pruebas periódicas de recuperación, asegurar que los respaldos estén protegidos frente a ataques y, sobre todo, capacitar constantemente a los equipos.