EL MERCURIO

Fecha: 05/08/2025 Audiencia: 320.543 Sección: ESPECIALES
Vpe: $8.160.506 Tirada: 126.654 Frecuencia: 0
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 39,67%

SEGURIDAD INTEGRADA DESDE EL DISEÑO:

Data centers e infraestructura crítica

Ante el aumento de ciberataques en Latinoamérica, los data centers se consolidan como pilares de la infraestructura crítica nacional y corporativa. Integrar la ciberseguridad desde su diseño, junto con estrategias como Zero Trust y la colaboración público-privada, resulta clave para proteger los activos digitales más sensibles de las organizaciones.

IVÁN TORO,
CEO de ITQ Latam.

GROVTIKA - UNSPLASH

En materia de centros de datos, invertir en ciberseguridad puede evitar riesgos y daños por sumas mucho mayores que dicha inversión.

Son millones de ciberataques en Chile y América Latina cada año, y uno de los objetivos son los *data centers*: el corazón tecnológico de las organizaciones, donde almacenan, procesan y gestionan sus datos más sensibles. De ahí su relevancia en materia de ciberseguridad, la que radica en que estas imponentes máquinas centralizan los más importantes activos digitales, entre bases de datos, aplicaciones y servidores. Alojan información sensible, tanto comercial como de finanzas, contabilidad, inventarios, planes estratégicos, usuarios y *passwords*. Su disponibilidad y protección son fundamentales para la continuidad operativa.

En Santiago de Chile se encuentra la mayor parte de los *data centers* que almacenan información valiosa, no solo de empresas y organizaciones a nivel local, sino también de toda la región. Los *data centers*, como primera línea de defensa para la infraestructura crítica, contienen los sistemas que controlan servicios esenciales: energía, agua, telecomunicaciones, salud o defensa. Vulnerar uno de esos servicios puede impactar severamente en los servicios de infraestructura crítica. Los *data centers* pueden ser el punto de entrada o contención de muchas amenazas.

Lamentablemente, de la misma manera, los centros de datos son objetivos prioritarios para ciberataques (*ransomware*, DDoS), con el objetivo de alterar o robar información de las organizaciones o para llegar a otros sistemas conectados, pasando a través de estas plataformas.

En este escenario, los principales desafíos en ciberseguridad para un *data center* incluyen protección de las constantes amenazas de ciberseguridad (APT, ataques a *firmware*, IA maliciosa). También, gestión en forma segura del acceso físico y lógico al *data center*; cumplimientos normativos (ISO 27001, GDPR, leyes nacionales) que permitan bajar los riesgos físicos y lógicos, y la actualización continua del *software* y *hardware* alojados en los centros de datos.

CARACTERÍSTICAS CLAVE

Aunque comparten principios similares, la infraestructura crítica nacional incorpora servicios básicos que pueden impactar a toda la población, mientras que, en las infraestructuras corporativas, se trata de alcances e impactos más reducidos por tratarse de sistemas de compañías que impactan a los clientes de dichas empresas. No obstante, un *data center* destinado a proteger infraestructura crítica, ya sea a nivel nacional o corporativo, debe tener, a lo menos, las siguientes características clave:

- Redundancia en energía, conectividad y refrigeración (mínimo Tier III o IV).
- Controles de acceso físico robustos, como biometría, videovigilancia y zonas restringidas.
- Sistemas avanzados de detección y respuesta ante amenazas (SIEM, EDR, NDR).
- Segmentación de red y *firewalls next generation*.
- Monitoreo 24/7 con centros de disponibilidad (NOC) y gestión de seguridad (SOC).
- Planes de recuperación ante desastres (DRP) y de continuidad operativa (BCP).
- Auditorías y pruebas regulares de penetración (*pentesting*).
- Cumplimiento normativo y certificaciones internacionales (ISO, NIST, ENS).

ITQ LATAM

Iván Toro, CEO de ITQ Latam.

Con todo, lo cierto es que es sumamente importante entender que una inversión en ciberseguridad puede evitar riesgos y daños por sumas mucho mayores que la inversión. Por ello, es indispensable dar prioridad a la protección física y lógica de los *data centers*.

En ese contexto y con ese foco, lo ideal es que la seguridad sea *bydesign*, es decir, integrada desde el diseño del *data center*. Es clave también adoptar una postura de Zero Trust, lo que equivale a nunca confiar.

Finalmente, lo recomendable es fomentar la colaboración público-privada, especialmente en temas de infraestructura crítica.