LITORALPRESS

Fecha: 21-04-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Columnas de Opinión
Título: COLUMNAS DE OPINIÓN: Ciberseguridad: factor crítico para la continuidad operativa

Pág. : 5
Cm2: 430,3

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Ciberseguridad: factor crítico para la continuidad operativa

Héctor Garretón, gerente Comercial de Novared – www.novared.net

La acelerada digitalización de los procesos productivos y financieros ha dejado de ser una promesa de eficiencia para convertirse en una realidad ineludible. Sin embargo, este avance también ha traído consigo una exposición creciente a amenazas informáticas, posicionando a la ciberseguridad como un factor crítico para la continuidad operativa en sectores como banca, minería, energía, retail y salud.

El panorama de riesgos ha evolucionado de manera drástica. Atrás quedaron los ataques aislados de hackers individuales. Hoy enfrentamos a organizaciones criminales sofisticadas, algunas incluso vinculadas a redes de narcotráfico o terrorismo, que han encontrado en la tecnología un terreno fértil. Adicionalmente, la irrupción de la Inteligencia Artificial ha elevado aún más el nivel de amenaza, pues los atacantes ahora utilizan bots automatizados capaces de rastrear internet en busca de vulnerabilidades, las que luego son comercializadas en la Dark Web, dando forma a un ecosistema delictivo más escalable y difícil de contener.

Sin duda, este fenómeno ha democratizado el riesgo. Ya no se trata solo de grandes bancos o corporaciones globales. Hoy, cualquier organización- independiente de su tamaño o industria- puede ser blanco de ataques desde cualquier lugar del mundo.

En este contexto, sectores como la salud y la banca siguen siendo particularmente atractivos debido

al volumen y sensibilidad de los datos que manejan. En industrias como la energía, el petróleo o la minería, que operan con sistemas físicos conectados a redes digitales, un ataque no solo puede comprometer la información, sino también paralizar las operaciones. En minería, por ejemplo, la intervención maliciosa de camiones autónomos podría detener faenas completas, generando pérdidas millonarias. En retail o alimentos, una intrusión podría afectar la cadena de suministro y dañar gravemente la reputación de una marca.

Pese a este complejo escenario, existen avances. La banca chilena, por ejemplo, ha desarrollado estructuras robustas de protección. Sin embargo, el principal desafío actual no es solo tecnológico, sino también humano. Muchas brechas se originan en errores internos o en la falta de cumplimiento de protocolos.

Frente a ello, modelos como Zero Trust han cobrado relevancia, proponiendo un enfoque basado en la verificación constante de identidades y accesos. Asimismo, tendencias como BYOD amplían la superficie de ataque, obligando a reforzar la seguridad en todos los niveles.

La transformación digital, especialmente con la migración a la nube, ha incrementado los puntos vulnerables. Por ello, la ciberseguridad debe entenderse como una inversión estratégica, fundamental para la continuidad operativa. Un ataque no solo implica pérdida de datos, sino también interrupciones productivas y daño reputacional.

En Chile, la nueva Ley Marco de Ciberseguridad establece un punto de inflexión al exigir el reporte de incidentes, promoviendo mayor transparencia y mejores prácticas. Paralelamente, la misma Inteligencia Artificial que potencia los ataques también se perfila como aliada en la defensa, permitiendo detectar anomalías y anticipar amenazas.

Dado lo anterior, el desafío en las distintas verticales es reconocer que las ciberamenazas son una realidad permanente. Solo mediante una cultura organizacional sólida, inversión adecuada y estrategias preventivas será posible resguardar no solo los sistemas, sino también la confianza, un activo cada vez más valioso en la era digital.