LITORALPRESS

Fecha: 21-04-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Columnas de Opinión
Título: COLUMNAS DE OPINIÓN: Ciberseguridad 2026: Cuando la resiliencia operativa es la verdadera promesa ciudadana

Pág. : 4
Cm2: 448,4

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Ciberseguridad 2026: Cuando la resiliencia operativa es la verdadera promesa ciudadana

Carolina Eyquem, Responsable de Soluciones de Estrategia y Riesgo en SONDA

Cuando un sistema crítico falla, lo que el ciudadano percibe no es un error de código, sino una promesa incumplida. En una era de profunda integración digital, la ciberseguridad ha dejado de ser un asunto tecnológico para convertirse en el pilar que sostiene la operación diaria. Para una institución pública, un banco o un operador logístico, un incidente no es solo una brecha; es una fila que no avanza, un trámite crítico que se detiene o un servicio esencial que se cae cuando más se necesita, impactando directamente en la continuidad, el riesgo y la reputación.

Por lo tanto, la pregunta correcta en los directorios ya no es "¿estamos protegidos?", sino "¿podemos seguir operando bajo ataque y recuperar el servicio con rapidez y control?".

Este cambio de paradigma está respaldado por la evolución regulatoria. En Chile, la Ley Marco de Ciberseguridad N° 21.663 nos exige entender esta disciplina como una obligación de gestión de riesgos y respuesta, especialmente para servicios esenciales y operadores de importancia vital. En paralelo, marcos internacionales como NIST CSF 2.0 elevan la gobernanza del riesgo cibernético al nivel directivo. Dicho de forma simple: la ciberseguridad dejó de ser un catálogo de controles para convertirse en un componente formal del gobierno corporativo.

La evidencia global es contundente. El ransomware y las intrusiones a sistemas siguen siendo amenazas dominantes, presentes en el 39% de las brechas en grandes organizaciones, según el reporte Verizon DBIR 2025. Y si bien el impacto financiero es severo, con un costo que promedia los USD 4,4 millones por incidente a nivel global, el daño más profundo y persistente es el reputacional. Cada hora de indisponibilidad quiebra la confianza ciudadana, un activo que no se recupera con un simple comunicado.

Por eso, la ciberseguridad efectiva debe entenderse como un programa continuo de resiliencia, articulado en tres capas inseparables:

Primero, la preparación. Identificar los procesos críticos que sostienen la atención y el servicio, y definir tolerancias de operación. Esto implica diseñar escenarios de crisis reales para sostener el servicio durante una disrupción, alineándose con estándares de continuidad.

Segundo, la detección y respuesta. Se requiere visibilidad 24/7 y la capacidad de contener amenazas con playbooks probados. No hablamos de documentos guardados en un cajón, sino de práctica constante y simulación.

Y, en tercer lugar, la recuperación. Contar con respaldos inmutables, segregación de redes y una verificación exhaustiva de integridad antes de volver a producción. Si esta capa falla, la organización queda expuesta al peor escenario: restaurar los sistemas rápido, pero volver a ser vulnerados.

Cuando se entiende bajo esta mirada integral, la ciberseguridad se convierte en una promesa pública: no fallarle a la ciudadanía. En un 2026 donde la superficie de ataque ha crecido por la nube híbrida y la IA, el liderazgo debe transitar desde una medición basada en herramientas adquiridas, hacia una enfocada en capacidades operativas concretas, como los tiempos de detección, contención y recuperación. Esa combinación de exigencias regulatorias y operacionales vuelve inevitable un cambio cultural. Requiere líderes y dueños de procesos que entiendan que la continuidad operacional demostrable, y no la seguridad declarativa, es lo que respalda el prestigio de la organización.

El mensaje es claro, en la era digital la reputación se sostiene en la continuidad. Si bien la robustez del SOC y los controles técnicos son cimientos indispensables, la ciudadanía mide el éxito en la respuesta final, si el servicio funciona, si su información está a salvo y si, ante un incidente, la institución responde con transparencia y rapidez. La tecnología es el gran habilitador, pero la diferencia la hace la gestión estratégica: gobernanza, operación y resiliencia. Si esta tríada está bien diseñada, la ciberseguridad se convierte en la capacidad estratégica más valiosa: proteger la confianza y mantener en pie la promesa fundamental de toda institución moderna.