LITORALPRESS

Fecha: 12-05-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Columnas de Opinión
Título: Columnas de Opinión: Ciberseguridad: de escudo técnico a habilitador del negocio digital

Pág. : 4
Cm2: 391,7
VPE: $ 783.485

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Ciberseguridad: de escudo técnico a habilitador del negocio digital

La ciberseguridad dejó de ser una conversación confinada a las áreas técnicas. Cuando todo está marcado por inteligencia artificial (IA), cadenas digitales interconectadas y mayor exposición operativa, hoy cumple una función mucho más estratégica: habilitar que el negocio digital opere con confianza, continuidad y capacidad de adaptación. El "Global Cybersecurity Outlook 2026" del World Economic Forum, elaborado en colaboración con Accenture, advierte que la aceleración de la IA, la fragmentación geopolítica y la creciente interdependencia digital están reconfigurando el mapa global de riesgo y aumentando la presión sobre organizaciones y gobiernos para adaptarse.

Ese cambio es relevante porque modifica la pregunta de fondo. Ya no basta con pensar la ciberseguridad como una barrera para contener incidentes. Hoy debe entenderse como una capacidad que permite sostener operaciones seguras, ágiles y confiables en entornos cada vez más complejos. Cuando una organización depende de plataformas conectadas, datos distribuidos, ecosistemas de terceros y decisiones en tiempo real, la seguridad deja de ser un tema periférico: pasa a ser parte del diseño mismo de la operación.

Entonces, la resiliencia y la continuidad operacional adquieren un nuevo peso. No se trata solo de prevenir ataques, sino de asegurar que la organización pueda anticipar, responder y recuperarse sin comprometer su capacidad de servir a clientes, operar procesos críticos o capturar valor. La competitividad futura dependerá crecientemente de la capacidad de las industrias para integrar tecnología, datos y colaboración estratégica, construyendo organizaciones más adaptables e inteligentes frente a la disrupción.

La urgencia es concreta. Según el reporte "State of Cybersecurity Resilience 2025" de Accenture, solo 36% de los líderes tecnológicos reconoce que la IA está avanzando más rápido que sus capacidades de seguridad, mientras 90% de las organizaciones no tiene la madurez necesaria para defenderse de amenazas modernas potenciadas por IA. El mismo estudio revela que 77% carece de prácticas fundamentales de seguridad de datos e IA, y que apenas 28% incorpora seguridad desde el inicio de sus iniciativas de transformación.

Eso confirma que el principal riesgo no está solo en la sofisticación del atacante, sino también en la distancia entre la velocidad de la transformación digital y la preparación real de las organizaciones para sostenerla con seguridad. Cuando la ciberseguridad entra tarde, se vuelve un factor de fricción. Cuando se integra desde el diseño, se transforma en un habilitador del negocio: acelera

María Luisa Acuña, Managing Director Cybersecurity de Accenture Chile

decisiones, protege activos críticos, fortalece la confianza y reduce la exposición de la operación ante interrupciones con impacto reputacional, financiero y operacional.

Por eso, la conversación ejecutiva debe cambiar. La ciberseguridad no puede seguir evaluándose solo por su capacidad de bloquear amenazas, sino también por su aporte a la resiliencia del negocio. En la práctica, eso exige integrar seguridad, datos, IA, operaciones y continuidad bajo una misma lógica estratégica. Porque en la economía digital, competir no dependerá únicamente de cuánto se innova, sino de cuán preparado se está para sostener esa innovación con confianza. La resiliencia ya no es una respuesta defensiva. Es una condición para crecer.