GERENCIA
Tecnologías y estrategias para la transformación digital

Fecha: 30/03/2026 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $694.918 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $829.080 Difusión: 0
Vpe portada: $829.080 Ocupación: 83,82%

El mayor factor de cambio de la ciberseguridad en 2026

La inteligencia artificial se consolida como el principal factor de transformación en ciberseguridad, ampliando la superficie de ataque y elevando la sofisticación de las amenazas, pero también potenciando las capacidades de defensa. Este nuevo escenario obliga a las organizaciones a equilibrar automatización, gobernanza y supervisión humana para gestionar los riesgos asociados a su adopción.

Por María Luisa Acuña, Cybersecurity Lead de Accenture Chile.

La inteligencia artificial será el factor de cambio más significativo en ciberseguridad durante este año. Así lo previó el 94% de los ejecutivos encuestados a nivel mundial por el World Economic Forum (WEF) y Accenture, en la última versión de su estudio, Global Cybersecurity Outlook. La inteligencia artificial está reconfigurando el panorama de la ciberseguridad y, por tanto, desafiando a las organizaciones a repensar sus estrategias y modelos de operación de ciberseguridad. En este sentido, hay tres dimensiones interconectadas:

1. La integración generalizada de sistemas de IA introduce una superficie de ataque ampliada, creando vulnerabilidades novedosas que los controles tradicionales no fueron diseñados para abordar.

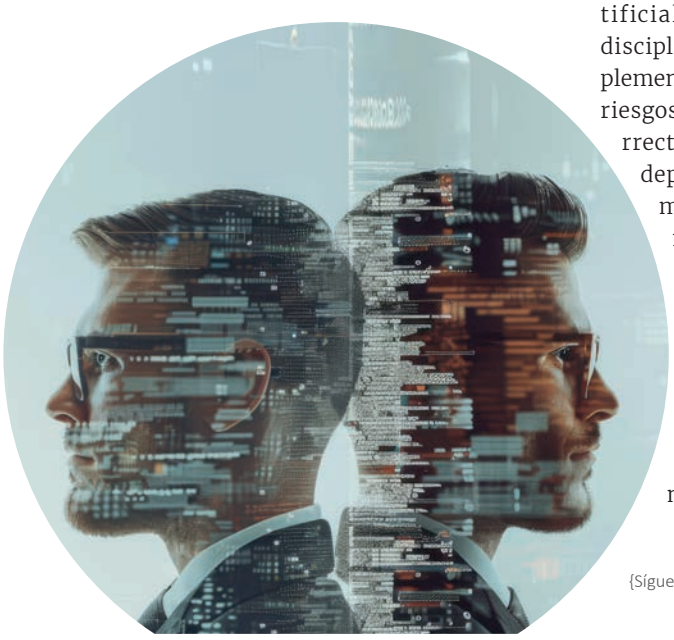
2. Los defensores están aprovechando la IA para fortalecer sus capacidades cibernéticas, mejorando la detección, acelerando la respuesta a incidentes y automatizando tareas analíticas de alto volumen.

3. Los ciberatacantes están utilizando la IA para aumentar la escala, velocidad, sofisticación y precisión de sus ataques, impulsando una nueva generación de ingeniería social dirigida.

En conjunto, estas dinámicas ilustran la naturaleza de doble uso de la IA, tanto como un multiplicador de fuerza para la defensa como un catalizador para los atacantes. A medida que esta competencia tecnológica se intensifica, las organizaciones están transitando desde un enfoque de seguridad reactivo hacia uno proactivo, al tiempo que reevalúan la gobernanza, la validación y la supervisión en cada etapa de la adopción de la IA.

Los riesgos de la IA

Los beneficios de la inteligencia artificial dependen de una ejecución disciplinada. Las soluciones mal implementadas pueden introducir nuevos riesgos -como configuraciones incorrectas, toma de decisiones sesgada, dependencia excesiva de la automatización y susceptibilidad a manipulaciones adversarias- a menos que las organizaciones incorporen salvaguardas sólidas, prácticas de seguridad desde el diseño (security-by-design) y monitoreo continuo. La encuesta también reflejó como algunas organizaciones ya están avanzando en



un aseguramiento continuo de sus herramientas de IA. El 40% informó que realizan revisiones periódicas de sus herramientas de IA antes de desplegarlas, en lugar de realizar únicamente una evaluación única (24%). Sin embargo, aproximadamente un tercio todavía carece de cualquier proceso para validar la seguridad de la IA antes de su despliegue, lo que deja exposiciones sistémicas incluso mientras se acelera la carrera por adoptar la IA en las ciberdefensas.

La implicancia es clara: la IA puede mejorar la ciberseguridad, pero solo cuando se despliega dentro de marcos de gobernanza robustos que mantengan el juicio humano en el centro. Al mismo tiempo, un exceso de controles puede generar fricción, por lo que resulta esencial encontrar un equilibrio cuidadoso.

¿Estamos preparados para la IA?

El impulso del mercado por incorporar nuevas funcionalidades de IA suele superar el nivel de preparación en materia de seguridad, creando vulnerabilidades explotables. En respuesta a estos riesgos emergentes, debería priorizarse una serie de medidas fundamentales para asegurar la IA a nivel de infraestructura. Esto incluye

El impulso del mercado por incorporar nuevas funcionalidades de IA suele superar el nivel de preparación en materia de seguridad, cr

proteger los datos utilizados en el entrenamiento y la personalización de los modelos de IA frente a filtraciones y accesos no autorizados. Los sistemas de IA deben desarrollarse con la seguridad como principio central, incorporando actualizaciones y parches periódicos para abordar posibles vulnerabilidades. Asimismo, es fundamental que las organizaciones implementen protocolos robustos de autenticación y cifrado para garantizar la protección de las interacciones y los datos de los clientes.

A medida que las organizaciones avanzan en la integración de la inteligencia artificial en sus operaciones de seguridad, el equilibrio entre la automatización y el juicio humano se vuelve cada vez más crítico. Si bien la IA destaca en la automatización de tareas repetitivas y de alto volumen, sus limitaciones actuales en materia de juicio contextual y toma de decisiones estratégicas siguen siendo evidentes. La dependencia excesiva de una automatización sin una adecuada gobernanza corre el riesgo de crear puntos ciegos que los adversarios pueden explotar. Al abordar los desafíos prácticos de la adopción de la IA en ciberseguridad, las organizaciones identifican de manera consistente la falta de conocimientos y/o habilidades suficientes (54%) para desplegar la IA, la necesidad de supervisión humana (41%) y la incertidumbre sobre el riesgo (39%) como los principales obstáculos. Estos hallazgos indican que la confianza sigue siendo una barrera para la adopción generalizada de la IA.

Las prioridades para las organizaciones este 2026 son claras: invertir en alfabetización en IA y en habilidades para su uso seguro, e integrar mecanismos de gobernanza y validación, sin crear nuevos puntos únicos de falla. Un modelo colaborativo, anclado en principios de seguridad desde el diseño (security-by-design), surge como el camino recomendado hacia adelante, permitiendo a las organizaciones aprovechar las ventajas de la IA mientras mitigan vulnerabilidades y aseguran que la innovación fortalezca -y no comprometa- la ciberseguridad. **G**