LITORALPRESS

Fecha: 22-04-2026
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Noticia general
Título: **Velocidad, integración y aprendizaje continuo como claves del nuevo escenario**

Pág. : 3
Cm2: 570,2

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CIBERSEGURIDAD EN TIEMPOS DE IA:

Velocidad, integración y aprendizaje continuo como claves del nuevo escenario

El avance de la inteligencia artificial redefine los riesgos y las defensas digitales. Por ello, desde Fortinet, advierten sobre la urgencia de consolidar plataformas, acelerar decisiones y adoptar modelos que aprendan en tiempo real.

La irrupción de la inteligencia artificial (IA) está reconfigurando de manera profunda el panorama de la ciberseguridad a nivel global. En América Latina y Chile, este fenómeno no solo amplifica los riesgos, sino que también abre nuevas oportunidades para fortalecer las defensas. Sin embargo, el principal desafío radica en la velocidad: mientras las amenazas evolucionan rápidamente, las organizaciones avanzan con una inercia que ya no es sostenible.

"Los temas de inteligencia artificial cambian significativamente la película, tanto desde el punto de vista del riesgo como de la defensa", afirma Pedro Paixao, senior VP de ventas para Fortinet en Latinoamérica, el Caribe y Canadá. Según explica, hoy las empresas cuentan con herramientas más avanzadas que permiten automatizar procesos, mejorar la productividad de los equipos de seguridad y acelerar la respuesta ante incidentes. Pero, al mismo tiempo, los atacantes utilizan las mismas tecnologías, lo que genera un escenario más complejo y competitivo.

Uno de los cambios más relevantes es la llamada "democratización del ataque". Paixao advierte que la sofisticación ya no depende exclusivamente del conocimiento del cibercriminal, sino de las herramientas que utiliza. "La inteligencia ya no está en el criminal, está en la herramienta, entonces cualquiera la puede usar", señala. Esto se traduce en ataques más automatizados, frecuentes y difíciles de detectar.

FORTINET

Joao Horta, SR VP para Service Providers para Fortinet Latinoamérica, Caribe y Canadá; Andrés Pérez, VP de Ventas para Fortinet Chile; Jenny Zamudio, VP de Servicios de Ciberseguridad para Fortinet Latinoamérica, Caribe y Canadá; Pedro Paixao, SVP de Ventas para Latinoamérica, el Caribe y Canadá para Fortinet; Gonzalo García, VP de Ventas para Fortinet Sudamérica, y Leandro Reyes, VP de Ingeniería en Sistemas para Fortinet Chile.

FORTINET

Pedro Paixao, senior VP de ventas para Fortinet en Latinoamérica, el Caribe y Canadá.

DESAFÍOS

A este escenario se suma una debilidad estructural en muchas organizaciones: la fragmentación de sus sistemas de seguridad. Durante años, las empresas han adquirido soluciones de forma aislada, generando entornos con múltiples herramientas que no se comunican entre sí. "Estamos hablando de 20 o 30 años de construir infraestructura con sistemas que no están integrados. Eso deja espacios sin visibilidad, mientras el atacante sí la tiene completa", explica.

Esta falta de integración no solo aumenta la exposición al riesgo, sino que también dificulta la implementación efectiva de la inteligencia artificial. En un contexto donde, según estimaciones de la industria, una empresa promedio puede tener decenas de soluciones de seguridad, la incorporación de IA sin una estrategia unificada puede profundizar el problema en lugar de resolverlo.

Otro desafío es el desconocimiento sobre el funcionamiento de la IA. Paixao advierte que muchas organizaciones fallan en sus proyectos porque intentan aplicar estos modelos en procesos que requieren resultados determinísticos. "Son modelos estadísticos. No siempre entregan la misma respuesta, y hay procesos empresariales que no pueden ser así", explica. Esta característica introduce una nueva variable de riesgo que exige mecanismos de validación y control más sofisticados.

En este contexto, la propuesta de valor de Fortinet se centra en la consolidación y la construcción de plataformas integradas. La compañía apuesta por un enfoque donde la ciberseguridad funcione como un ecosistema, capaz de operar a la velocidad de la máquina y no de los procesos humanos. "La estrategia es detectar, proteger y aprender en un ciclo continuo. Solo así podemos responder a la velocidad de los ataques actuales", sostiene Paixao.

Un elemento clave de esta visión es el uso de agentes de inteligencia artificial capaces de tomar decisiones y ejecutar acciones en tiempo real. Estos agentes no solo apoyan a los equipos de seguridad, sino que también pueden actuar directamente sobre la infraestructura, reduciendo tiempos de respuesta y minimizando errores humanos. "Vamos hacia un modelo donde la IA no solo recomienda, sino que actúa", enfatiza.

Asimismo, la compañía impulsa la adopción de modelos de seguridad más simples y unificados, como las arquitecturas SASE y plataformas de operaciones de seguridad (SecOps) integradas. El objetivo es reducir la complejidad, mejorar la visibilidad y permitir una gestión más eficiente de los riesgos.

Paixao también subraya la importancia de la concientización a nivel ejecutivo. Muchas decisiones, dice, aún se toman en función de cumplir auditorías y no de mejorar realmente la seguridad. "Se gasta dinero y se cree que se está seguro, pero no necesariamente es así", advierte. En este sentido, plantea que la ciberseguridad debe ser entendida como un pilar estratégico, al mismo nivel que otras prioridades críticas del negocio o del Estado.

Finalmente, el ejecutivo destaca que la transformación no solo es tecnológica, sino también cultural. La capacitación continua, el rol de los socios tecnológicos y la colaboración entre actores del ecosistema serán determinantes para enfrentar este nuevo escenario.

"La seguridad es confianza", concluye. Y en un entorno donde la inteligencia artificial redefine las reglas del juego, construir esa confianza dependerá de la capacidad de las organizaciones para adaptarse, integrar y aprender más rápido que las amenazas.