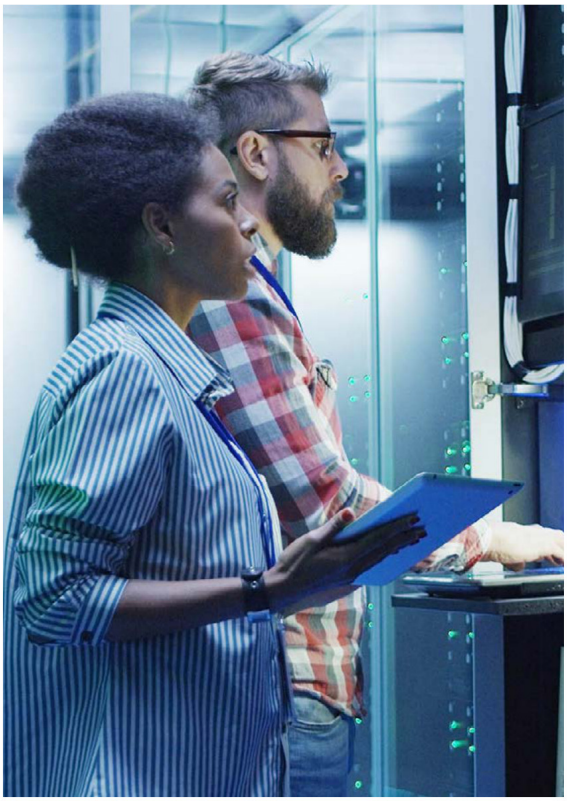
El Rancagüino
El Diario de la Región de O'Higgins
Fecha: 14/03/2026 Audiencia: 15.000 Sección:
Vpe: $1.506.002 Tirada: 5.000 Frecuencia: 0
Vpe pág: $1.606.745 Difusión: 5.000
Vpe portada: $1.606.745 Ocupación: 93,73%

IA DELICTIVA: ALGORITMOS FUERA DE LA LEY



Daniel Galilea / EFE – Reportajes

La inteligencia artificial o IA se ha convertido en un eje central del mundo de la ciberseguridad, y la dualidad de su utilización, con fines protectores, por un lado, y delictivos, por otro, plantea una carrera armamentista digital en la que conviven sistemas defensivos altamente avanzados con herramientas ofensivas igualmente sofisticadas, según expertos consultados por EFE.

No estamos viendo una simple escalada tecnológica, sino un cambio de paradigma absoluto en la ciberseguridad, enfatizan.

"La inteligencia artificial se ha convertido en un eje central del panorama de la ciberseguridad, y su dualidad plantea un nuevo modelo: una especie de carrera armamentista digital en la que conviven sistemas defensivos altamente avanzados con herramientas ofensivas igualmente sofisticadas", señala Mario García, director general para España y Portugal de la firma de ciberseguridad Check Point Software (www.checkpoint.com).

En ese sentido "observamos un enfrentamiento cada vez más complejo entre lo que podríamos definir como 'IA defensiva' e 'IA ofensiva'", explica García.

Explica que la 'inteligencia artificial que defiende', integrada en plataformas de ciberseguridad avanzadas, "utiliza decenas de motores de análisis basados en IA para detectar, prevenir y responder en

continúa

El Rancagüino
El Diario de la Región de O'Higgins

Fecha: 14/03/2026 Audiencia: 15.000 Sección:
Vpe: $1.447.035 Tirada: 5.000 Frecuencia: 0
Vpe pág: $1.606.745 Difusión: 5.000
Vpe portada: $1.606.745 Ocupación: 90,06%

EN EL ÁMBITO DE LA CIBERSEGURIDAD SE DESARROLLA UN 'DUELO DE GIGANTES' ENTRE LA INTELIGENCIA ARTIFICIAL AL SERVICIO DE LA PROTECCIÓN DE LOS SISTEMAS Y LA QUE SE UTILIZA PARA VULNERARLOS. ¿PUEDE HABER UN GANADOR EN ESTA GUERRA ENTRE UNAS IAS QUE PODRÍAN ALCANZAR UNA INTELIGENCIA SUPERIOR A LA HUMANA Y SER CAPACES DE MEJORARSE A SÍ MISMAS? NO HAY UNA RESPUESTA DEFINITIVA, SEGÚN LOS EXPERTOS.

tiempo real a amenazas emergentes, incluyendo malware polimórfico (programas maliciosos que pueden modificar su propio código para cambiar su 'apariencia'), 'deepfakes' (videos ultrafalsos) y ataques automatizados".

Un exponente de esta tecnología es el sistema de ciberseguridad Check Point Infinity ThreatCloud AI, puntualiza.

Además, "la IA generativa defensiva actúa como copiloto de seguridad para asistir a los analistas en tareas complejas, reducir los tiempos de respuesta y anticipar movimientos del adversario", añade.

FRAUDGPT Y WORMGPT: EL PELIGRO DE LAS IA NO ÉTICAS

Pero García advierte que, a su vez, "los ciberdelincuentes están replicando estos avances mediante el uso de IAs generativas no éticas como FraudGPT o WormGPT, capaces de generar campañas de 'phishing' (suplantación de identidad) altamente convincentes, contenido manipulado, ingeniería social automatizada y 'malware' (programas maliciosos) adaptativo, todo ello con una mínima intervención humana".

"La descentralización de sus operaciones delictivas y la facilidad de acceso a modelos generativos de IA no filtrados aumentan su capacidad de ataque", enfatiza.

García anticipa que "a medio y largo plazo, en la ciberseguridad se producirá una evolución hacia ecosistemas híbridos de defensa autónoma, donde la IA no solo detecte, sino también actúe en tiempo real (instantáneamente) con decisiones inteligentes", lo cual "conllevará una redefinición de los actuales Centros de Operaciones de Seguridad (SOC)".

"La clave para mantener la ventaja sobre la ciberdelincuencia estará en la capacidad de combinar una IA explicable con la supervisión humana, reforzar la gobernanza de datos, y establecer un marco normativo global que limite el uso malicioso de estas tecnologías emergentes", según este especialista.

"La hipótesis de una superinteligencia autónoma en ambos frentes (el defensivo y el ofensivo) plantea un desafío filosófico, técnico y ético de gran magnitud", según García.

"En la práctica, el equilibrio entre estas dos fuerzas dependerá no solo de la capacidad técnica de las IAs, sino de cómo las sociedades, gobiernos y empresas logren establecer mecanismos de control, transparencia y supervisión responsables", opina.

EL ÉXITO DE LA IA DEFENSIVA DEPENDE DE TRES FACTORES

Desde Check Point Software creen que sería posible inclinar la balanza a favor de la IA defensiva, si se pusiera en marcha un liderazgo regulatorio global que establezca límites claros al uso de IA y prohíba aplicaciones como la manipulación del comportamiento, así como la evaluación y puntuación de individuos o grupos basándose en su comportamiento social.

"También sería determinante que se ponga en funcionamiento una gobernanza ética de la IA, que garantice que las empresas apliquen principios de diseño responsable, evitando sesgos, auditando modelos, protegiendo la privacidad y fomentando la supervisión humana", añade García.

"El éxito de la IA defensiva también dependerá de la colaboración público-privada y la ciberinteligencia colectiva, basada en redes globales de información compartida, como la que permite la plataforma ThreatCloud AI, capaz de analizar más de 2.000 millones de decisiones diarias a partir de datos de más de 150.000 redes y millones de dispositivos", asegura.

Señala que "no se trata de esperar un vencedor absoluto, sino de construir un ecosistema de ciberseguridad en el que la IA potencie la resiliencia (adaptación y resistencia), automatice la protección y preserve la confianza digital, limitando el uso destructivo de la inteligencia artificial".

"La IA no reemplazará al ser humano en la ciberseguridad, pero sí que lo potenciará. Y ese será el factor decisivo para prevalecer en esta guerra", concluye García, de Check Point Software.

INMERSOS EN UNA BATALLA ALGORÍTMICA

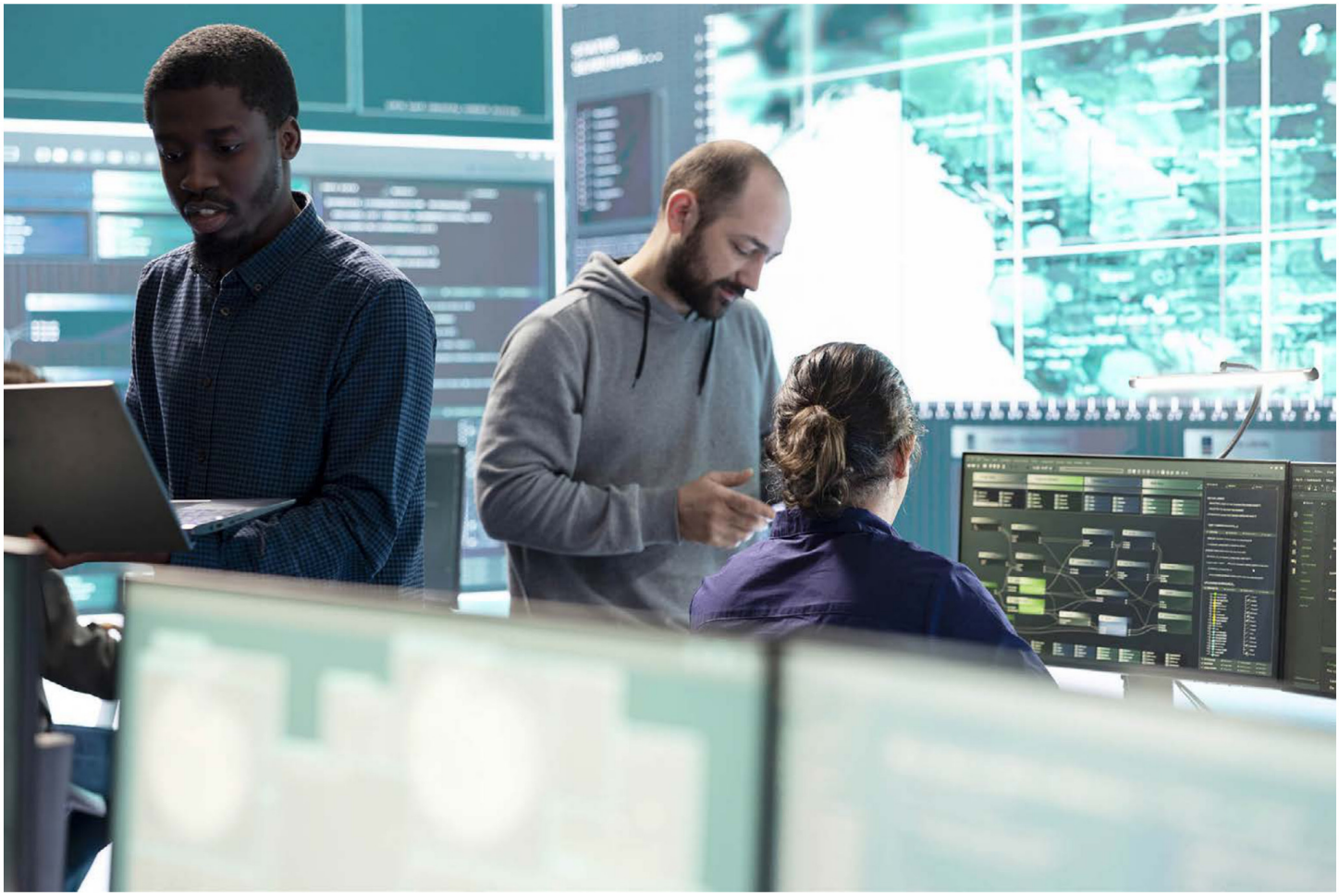
"Lo que estamos viendo actualmente no es una simple escalada tecnológica, sino un cambio de paradigma absoluto en el terreno de la ciberseguridad", señala a EFE, Pablo Chapinal, director regional en Iberia de Zscaler (www.zscaler.com), firma proveedora de seguridad empresarial en la nube.

"Estamos inmersos en una auténtica batalla algorítmica, donde las IAs juegan un papel fundamental tanto en el refuerzo de la protección de las empresas como en la sofisticación de las amenazas", puntualiza.

Chapinal señala que desde Zscaler observan cómo "las IAs al servicio del ciberdelito han ganado terreno gracias a su capacidad para

continúa

El Rancagüino
El Diario de la Región de O'Higgins
Fecha: 14/03/2026 Audiencia: 15.000 Sección: LOCAL
Vpe: $1.255.029 Tirada: 5.000 Frecuencia: 0
Vpe pág: $1.606.745 Difusión: 5.000
Vpe portada: $1.606.745 Ocupación: 78,11%



automatizar ataques a escala masiva, crear `malware´ (programas maliciosos) sofisticado e incluso explotar vulnerabilidades en tiempo real".

Además, los ciberdelincuentes "son capaces de operar con técnicas de evasión cada vez más avanzadas", ratifica.

Por su parte, la IA defensiva ha evolucionado para ofrecer una seguridad predictiva y contextual, que se apoya en volúmenes de datos inmensos y en arquitecturas 'zero trust' (estrategia de ciberseguridad que se basa en "nunca confiar, siempre verificar") integradas 'en la nube' (acceso y uso de recursos informáticos a través de internet, en vez de tenerlos físicamente).

Chapinal explica que en Zscaler procesan más de 500.000 millones de transacciones diarias, lo que alimenta a sus IAs defensivas con una visibilidad global sin precedentes. "Esta tecnología de inteligencia es clave para anticipar amenazas, y no solo reaccionar ante ellas", destaca.

Añade que el duelo o lucha entre las IAs "se está desplazando hacia un terreno donde la automatización, velocidad y capacidad de aprendizaje autónomo marcarán la diferencia".

LA IMPORTANCIA DEL ENFOQUE 'ZERO TRUST'

En el futuro, el éxito en este duelo no se sustentará en "tener mejores reglas o más analistas de ciberseguridad, sino en contar con una IA defensiva con enfoque 'zero trust' que aprenda, se adapte y actúe antes de que el ataque se materialice", enfatiza.

Consultado sobre si en esta guerra de IAs podría llegar a haber un ganador, Chapinal responde que "cuando hablamos de IA aplicada a la ciberseguridad, especialmente en el contexto de sus capacidades evolutivas o de superinteligencia, debemos asumir que no existe una solución definitiva ni una victoria absoluta"."La ciberseguridad no es un destino, sino un proceso continuo de adaptación y resiliencia", sentencia.

"Si bien es cierto que tanto las IAs defensivas como las ofensivas pueden alcanzar niveles de sofisticación superiores a la capacidad humana, la diferencia estará en el modelo operativo y el entorno en el que estas inteligencias se despliegan", explica Chapinal.

Añade que "las IAs maliciosas están sujetas a restricciones operativas: deben ocultarse, evadir controles y actuar sin ser detectadas".

En cambio, "la IA defensiva, cuando está integrada en una infraestructura global, legal y colaborativa tiene acceso a información masiva y en tiempo real, con capacidad para actuar desde el núcleo mismo de la conectividad empresarial", enfatiza.

"La clave no reside únicamente en quién tenga la IA más avanzada, sino en quién tenga la arquitectura adecuada para sostenerla, escalarla y adaptarla de forma segura", recalca.

En ese sentido, "el enfoque 'zero trust' es esencial, ya que elimina cualquier suposición de confianza implícita y permite una evaluación continua y granular de cada acceso y cada flujo de datos", concluye el experto de Zscaler.