TENDENCIAS EN CIBERSEGURIDAD PARA EL 2026

Progress. Protected.

TABLA DE CONTENIDOS

INTRODUCCIÓN

El panorama de ciberseguridad en América Latina sigue mostrando una creciente complejidad, con amenazas más sofisticadas y dirigidas hacia sectores públicos y privados. El ESET Security Report 2025 reveló que el 27% de las organizaciones de la región sufrió un ciberataque en el año previo, mientras que un 32% reconoció no contar con la visibilidad necesaria para confirmar si ha sido atacada, una brecha crítica que limita la capacidad de detección y respuesta.

A su vez, los accesos indebidos a sistemas y el robo de información sensible continuaron siendo las principales preocupaciones para las empresas. Además, el ransomware estuvo presente como una de las amenazas centrales, señalado por el 95% de los especialistas y con un 22% de organizaciones afectadas en los últimos dos años.

En este contexto, desde el Laboratorio de Investigación de ESET Latinoamérica analizamos tres tendencias que consideramos que marcarán el ritmo del año y alentamos a que sean tenidas en cuenta como parte de las estrategias a instaurarse para 2026 en las organizaciones. A lo largo del informe se abordarán los ejes temáticos que hemos considerado relevantes y que avizoramos que serán principales este año.

Por un lado, el ransomware, como viejo conocido, avanzará —o continuará su aceleración— hacia modelos cada vez más automatizados y lucrativos, con mayor profesionalización e industrialización a partir de del surgimiento de malware basado en inteligencia artificial.

La tendencia preponderante aquí, y de surgimiento reciente, indica que el uso ofensivo de la IA masificará la capacidad de generar contenido falso, campañas de fraude personalizadas y ataques autónomos. Un cóctel que desafía hoy mismo la velocidad de respuesta de las organizaciones, que deberán enfrentarse a nuevos vectores de riesgo, especialmente en cadenas de suministro.

En contrapartida la IA también se consolidará como herramienta clave para la detección temprana y la automatización defensiva.

Todo esto ocurre en un contexto en el que las regulaciones en el uso de inteligencia artificial pueden considerarse aún insuficientes en la región latinoamericana, donde solo ocho países cuentan con estrategias formales de IA. Este panorama representará el desafío urgente de acelerar marcos de gobernanza, promover la transparencia algorítmica y fortalecer la cooperación internacional.

A través de este informe, invitamos a las empresas de Latinoamérica a sumergirse en el análisis de las principales tendencias de ciberseguridad en 2024, como forma de estar mejor preparadas para fortalecer las defensas digitales, anticiparse a amenazas emergentes y proteger el valioso patrimonio digital en un entorno cada vez más desafiante y sofisticado.

1

USO INTENSIVO DE IA Y AUTOMATIZACIÓN OFENSIVA

Mario Micucci
Security Researcher
ESET Latinoamérica

Martina López
Security Researcher
ESET Latinoamérica

La inteligencia artificial dejó de ser una temática propia de los laboratorios dedicados a las ciencias de la computación. Según un reporte presentado en septiembre de 2025 por el equipo de investigación económica de OpenAI y publicado como *Working Paper* del National Bureau of Economic Research (NBER), la cantidad de usuarios activos semanales de ChatGPT equivale aproximadamente al 10% de la población adulta mundial.

Esta consolidación se explica por una multiplicidad de factores: el aumento de los servicios y sistemas que incorporan IA de manera directa o indirecta, la madurez de las herramientas -lograda a prueba y error-, su capacidad para resolver necesidades o dolores de las personas, y su sencilla accesibilidad para usuarios no técnicos.

En el ámbito corporativo, la combinación de implementación de herramientas que usen IA y la automatización produjo un gran salto de eficiencia operativa que podría llegar a compararse en unos años a grandes desarrollos y adopciones tecnológicas, como la virtualización o la nube. Muchas organizaciones adoptaron estas tecnologías bajo un principio conocido como "AI first mindset": automatizar la mayor cantidad de procesos y luego construir los flujos de trabajo manuales necesarios.

El mundo de la ciberseguridad está en una etapa en donde la inteligencia artificial es tanto una herramienta de defensa como un amplificador de ataque. La automatización puede convertirse tanto en un diferencial estratégico como en un multiplicador de impacto de incidentes. La cuestión dejó de ser si debe o no utilizarse la IA para resolver ciertos problemas, sino cómo garantizar que su uso intensivo no genere más riesgos que beneficios.

USO DEL ORDEN MASIVO

La masificación del uso de aplicaciones que usan modelos de inteligencia artificial redujo la brecha de habilidades técnicas necesarias para producir contenido: desde pequeños *snippets* de código, hasta documentos complejos y ediciones audiovisuales. En contraparte, el aumento del contenido sintético podría tener un impacto cognitivo a la hora de incorporar información. Podemos adelantar que tendrá consecuencias en la confianza social y la percepción de autenticidad. Será constante, casi como acto reflejo, preguntarse "¿es esto un deepfake?".

Por otro lado, los datos personales, patrones de comportamiento y preferencias se volvieron inputs permanentes para los modelos de IA. Esto hará que el contenido generado sea cada vez más humano y adaptado a las expectativas individuales. En contraste serán también moneda corriente: la creación de posibles vectores de envenenamiento involuntario, filtrado de información sensible y propagación de errores y contenido riesgoso.

Dentro del mundo corporativo, la IA se convirtió en un copiloto estándar en múltiples profesiones, con o sin autorización de las organizaciones. Su uso indiscriminado, y difícil de controlar operativamente, genera riesgos que van más allá de la filtración de datos. Entre los más relevantes: la automatización de errores humanos y la toma de decisiones apoyadas en modelos opacos.

Más allá del uso malicioso, la IA implica riesgos inherentes que obligan a desarrollar una adopción responsable, coexistiendo en un entorno donde todos los actores, incluidos los adversarios, también la utilizan.

EL USO MALICIOSO DE LA IA

La democratización de la IA la pone a disposición de cualquier actor, incluidos aquellos con fines dañinos. Para 2026 veremos una evolución acelerada en tres grandes dimensiones:

Contenido falsificado y manipulación

Se intensificará la creación de contenido falsificado orientado a manipulación, desinformación y fraude. La clonación de voz, hoy posible con pocos segundos de audio, habilita llamadas que inducen transferencias, desbloqueos o crisis emocionales (como las falsas llamadas de secuestro). También potencia campañas de influencia más segmentadas, erosionando la confianza pública y dificultando la verificación periodística.

Automatización criminal a escala

En el universo de estafas y engaños, los centros de estafa —reclutamiento, coacción, call centers criminales— utilizarán cada vez más herramientas de IA para generar guiones, perfiles de víctimas y operaciones automatizadas. Crecerá el uso de modelos y "plugins" capaces de ejecutar tareas completas que antes requerían mayor intervención humana, reduciendo drásticamente la barrera técnica. Por ejemplo, para automatizar ataques de ransomware o realizar tareas de reconocimiento y exfiltración. Incidentes recientes muestran ya campañas coordinadas íntegramente por IA.

Delitos de mayor gravedad y uso militar

En último lugar, encontramos aquellas temáticas relacionadas a delitos de mayor gravedad y preocupaciones de estado. Herramientas como los sistemas de "nudify" y la generación de imágenes o videos no consensuados incrementaron el abuso digital, especialmente entre jóvenes, con efectos psicológicos y legales crecientes. A nivel geopolítico, los avances en navegación y reconocimiento impulsan la autonomía de drones y sistemas no tripulados, con riesgos asociados al uso malicioso por actores estatales o no estatales, y al potencial de daños colaterales.

AUTOMATIZACIÓN IMPULSADA POR IA: LA TENDENCIA TRANSVERSAL QUE MULTIPLICA EL RIESGO

Una de las tendencias más disruptivas es la automatización integral mediante IA. A diferencia de la generación aislada de contenido, los modelos actuales pueden actuar como operadores completos, encadenando tareas y ejecutándolas de forma autónoma.

Esta automatización:

- **Reduce las barreras de entrada** para atacantes sin conocimientos técnicos.
- **Multiplica la escala** de campañas maliciosas, operando 24/7.
- **Aumenta la velocidad** de prueba, adaptación y despliegue de ataques.
- **Permite servicios criminales "as-a-service"** accesibles para cualquier actor.

El riesgo central es la creación de ecosistemas delictivos autónomos, donde la IA no asiste al atacante: lo reemplaza.

IMPACTOS ESPERADOS

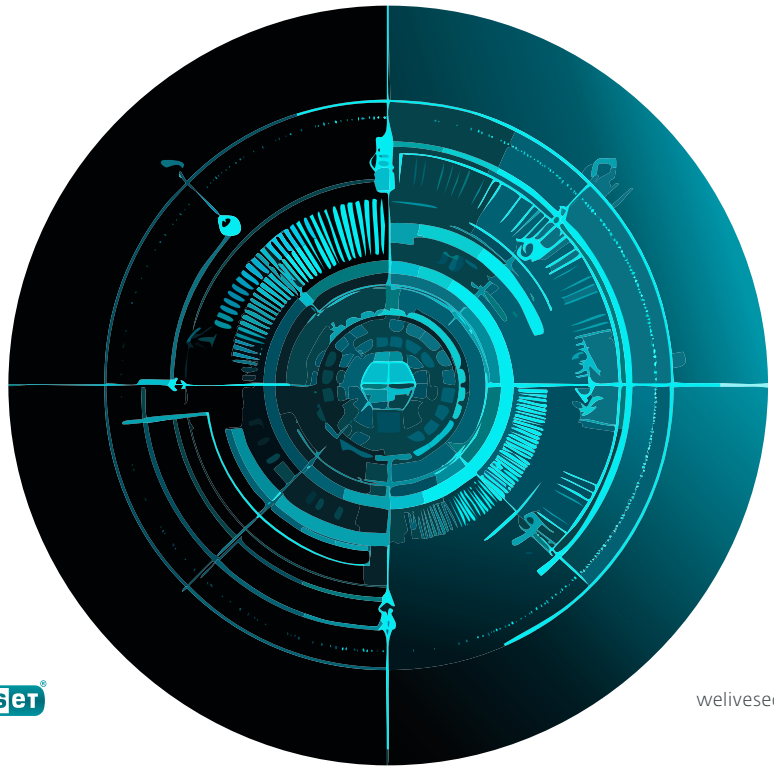
Así como la IA optimiza procesos legítimos, también hace más eficientes las operaciones delictivas: generación de código malicioso sin programadores, selección automatizada de víctimas sin analistas humanos, y correos de phishing extremadamente difíciles de detectar. Esto reduce costos para los atacantes y amplifica las pérdidas económicas de las víctimas.

Se profundizará, además, la **erosión de la confianza en internet**, especialmente en medios de comunicación y redes sociales. El crecimiento de aplicaciones generadoras de contenido sintético dificulta la verificación y afecta no solo al usuario promedio, sino también al periodismo, la justicia y otras instituciones que dependen de evidencia digital.

El 2026 será un **año bisagra** para comprender cómo los deepfakes, la automatización del acoso y la manipulación audiovisual influyen en relaciones personales, reputaciones y bienestar social.

Las organizaciones quedan atrapadas entre la necesidad de automatizar para ser más eficientes y la realidad de que los atacantes disponen de las mismas herramientas. Esta carrera entre velocidades de ataque y capacidades de respuesta genera presión permanente sobre equipos de seguridad.

La convergencia entre impactos económicos, sociales e institucionales será un desafío para todos los actores del ciberespacio: el daño económico erosiona la confianza social, la desinformación debilita instituciones y la falta de preparación profundiza las pérdidas corporativas.



2

LA EVOLUCIÓN DEL RANSOMWARE

Daniel Cunha Barbosa
Security Researcher
ESET Latinoamérica

El ransomware propiamente dicho es una amenaza con más de 30 años de existencia; aunque haya evolucionado con el tiempo, los ciberdelincuentes demostraron mayor interés y comenzaron a utilizarlo de forma más intensiva tras el surgimiento de las criptomonedas. Ese fue el principal hito en la historia de esta amenaza.

Desde entonces, el ransomware comenzó a tomar un papel destacado frente a otros tipos de malware, hasta llegar a la forma en que lo conocemos hoy. Con la adopción de activos digitales como forma de pago, el ransomware se convirtió en el principal método de monetización usado por los ciberdelincuentes, registrando más de 813 millones de dólares en pagos de rescate solo en 2024.

Esa cifra, además de permitir que los ataques de ransomware y otros tipos de amenazas continúen ocurriendo, posibilita que los grupos de ciberdelincuentes evolucionen cada vez más, en un ciclo vicioso que nos ha llevado a la realidad que enfrentamos hoy.

EL MODELO DE NEGOCIO DEL RANSOMWARE AS A SERVICE

Los grupos más experimentados de ciberdelincuentes se dieron cuenta de que tenían una posibilidad de ingresos bastante significativa con los ataques de ransomware en sí, pero que también podían monetizar de otras maneras: con otros delincuentes o individuos malintencionados.

Así fue que comenzaron a ofrecer piezas de software malicioso con garantía de que no serían detectados (FUD, Fully Undetectable), tutoriales, acceso a la infraestructura de gestión de víctimas, acceso a los servidores de comando y control (C2) e incluso soporte técnico.

Esto trajo dos efectos principales: un aumento de ingresos difícil de estimar por parte de los grandes grupos, y la capacitación de personas malintencionadas —ya sean otros ciberdelincuentes o individuos con poco o ningún conocimiento técnico ofensivo— para llevar a cabo ataques extremadamente bien estructurados, muchas veces pagando apenas unos cientos de dólares por ello.

Esta tendencia del RaaS está muy consolidada y sigue vigente: la gran mayoría de los grupos de ransomware en actividad adoptan este modelo y su eficacia a lo largo de los años ha incentivado a que nuevos actores de amenazas lo incorporen desde el inicio de sus actividades.

LA IA OFENSIVA COMO ACELERADOR DEL RANSOMWARE EN 2026

- Diversos análisis de ciberseguridad apuntan a que 2026 marcará un punto de inflexión en la evolución del ransomware. Esto tiene que ver con el impulso de la adopción de modelos de IA diseñados —o manipulados— para ejecutar tareas ofensivas de forma autónoma. IA tendrá la capacidad de automatizar desde el reconocimiento hasta la explotación en un nivel que antes requería equipos humanos especializados.

- Al menos una gran empresa podría ser comprometida por una IA agentiva capaz de planificar y ejecutar el ciclo completo del ataque, ajustándose en tiempo real y reduciendo la necesidad de operadores expertos detrás de las campañas.

- En este contexto, modelos potencialmente accesibles y orientados a tareas ofensivas —como *OpenClaw*— podrían convertirse en multiplicadores críticos del ransomware, no solo al generar variantes polimórficas y evadir defensas, sino también al automatizar el movimiento lateral, la exfiltración estratégica de datos y la negociación con las víctimas.

- Esta convergencia entre IA y RaaS habilita un escenario donde incluso actores con poca capacidad técnica pueden ejecutar ataques antes reservados a grupos con alto grado de sofisticación, acelerando la industrialización del cibercrimen y aumentando la presión sobre los defensores.

EVOLUCIÓN DEL MALWARE: PRIMER RANSOMWARE BASADO EN IA

A finales de agosto de 2025, el equipo de ESET Research descubrió PromptLock, un ransomware que marcó un hito al estar basado estructuralmente en IA. Por sus características, PromptLock fue considerado una prueba de concepto; aun así, arroja luz sobre una amenaza muy real y peligrosa.

A diferencia de las operaciones que desde principios de 2025 ya utilizaban la IA como apoyo para industrializar ataques, PromptLock sería el primer malware capaz de ejecutar un modelo de inteligencia artificial de forma local para generar código malicioso, seleccionar objetivos y decidir qué archivos cifrar o exfiltrar de forma autónoma y en tiempo real. Para ello, emplea scripts Lua, conocidos por su compatibilidad con varias plataformas como Windows, macOS y Linux.

Durante el análisis, fue posible identificar un módulo dedicado a la destrucción de archivos, aunque aún permanecía inactivo en la muestra analizada.
No es novedad que las IA están volviendo los ataques

cada vez más sofisticados, elaborados y accesibles, pero su uso como parte estructural de la amenaza agrega un nivel elevado de preocupación a la ecuación.

A través del uso de APIs, el malware podría acceder a modelos de lenguaje sofisticados, permitiendo que scripts maliciosos sean creados y entregados directamente en el dispositivo infectado, además de aportar una altísima capacidad de adaptación, mutación y evasión de defensas.

LA TRANSFORMACIÓN DEL BIG GAME HUNTING

Para abordar el último punto previsto en esta tendencia, es necesario mencionar al ransomware LunaLock. Para monetizar sus operaciones, este grupo adoptó un enfoque diferente respecto a las formas de extorsión más comunes, como la exigencia de pago de rescate para eliminar el cifrado, la doble extorsión —que amenaza con divulgar o vender los datos obtenidos— o la triple extorsión, que puede incluir ataques DDoS a activos importantes o incluso ataques a empresas asociadas de la víctima.

- En lugar de esto, tras atacar a la empresa Artists&Clients, el grupo informó que el rescate debía pagarse para evitar que todo el acervo de arte digital robado fuese utilizado para entrenar modelos de inteligencia artificial.

Aunque este ataque tuvo como objetivo a una empresa que sería gravemente afectada si sus obras alimentaran un modelo de IA generativa, el principal punto de atención está en el precedente que este tipo de enfoque establece. Es común que los ciberdelincuentes compartan Tácticas, Técnicas y Procedimientos entre sí y, aunque el ransomware haya sido la amenaza que abrió el camino a este método, es probable que otros tipos de malware que se beneficien de este modelo de extorsión lo adopten.

No tardaremos en ver IA generativas utilizadas para aportar innovaciones, mutaciones, nuevas funcionalidades o mecanismos de evasión de defensas a todos los tipos de malware conocidos, lo que hace imprescindible que los entornos también empleen tantos avances tecnológicos como sea posible para inhibir la acción de estas amenazas.

EL RANSOMWARE EN AMÉRICA LATINA: UN ESCENARIO CADA VEZ MÁS COMPLEJO

- El impacto del ransomware en América Latina durante 2025 dejó en evidencia que la región continúa siendo uno de los escenarios más activos del mundo para este tipo de ataques. Diversas investigaciones de WeLiveSecurity mostraron que variantes conocidas y nuevos actores delictivos concentraron esfuerzos en industrias sensibles de la región.

- La presión no se limitó a actores individuales: el ESET Security Report 2025, difundido en julio, confirmó que organizaciones de Argentina, Brasil, Chile y México —incluyendo universidades, hospitales y organismos gubernamentales— fueron blanco frecuente de variantes como LockBit, Medusa y RansomHub.

El reporte reveló, además, que 22% de las organizaciones de la región sufrió un ataque de ransomware en los últimos dos años, y que 95% de los especialistas de seguridad lo considera una de sus amenazas prioritarias. Sin embargo, menos de la mitad de estas instituciones implementaba controles de seguridad maduros, lo que refleja una brecha preocupante entre percepción y respuesta.

Finalmente, el informe también advirtió un problema estructural: incluso cuando 27% de las organizaciones declaró haber sufrido un ciberataque, un 32% reconoció no tener visibilidad para determinar si había sido atacada o no. Esta falta de monitoreo genera un terreno especialmente favorable para que familias como Medusa, LockBit o RansomHub operen con largas permanencias dentro de las redes corporativas.

CONCLUSIÓN

El panorama regional deja claro que, más allá del

avance tecnológico de las amenazas y que la IA seguirá siendo parte de su evolución, la falta de controles básicos tamién seguirá siendo un factor determinante que habilitará la expansión del ransomware en Latinoamérica durante 2026.

3

REGULACIÓN Y POLÍTICAS DE CIBERSEGURIDAD EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

David González
Security Researcher
ESET Latinoamérica

En los últimos años, la inteligencia artificial se ha convertido en un elemento central de la vida digital y la ciberseguridad: hoy potencia la detección temprana de amenazas, el análisis de grandes volúmenes de eventos y la anticipación de comportamientos maliciosos con mayor precisión. Este mismo avance, sin embargo, ha abierto la puerta a nuevos riesgos: campañas de phishing y BEC más verosímiles, deepfakes de voz utilizados para fraude, automatización de ataques y malware capaz de aprender y mutar.

La IA se consolida como un doble vector estratégico: fortalece la defensa digital, pero también amplifica las capacidades ofensivas. Por ello, la regulación ya no puede entenderse como un debate teórico, sino como un componente estructural de la gestión de riesgos y de la resiliencia organizacional.

Cualquier conversación seria sobre regulación en ciberseguridad estará inevitablemente atravesada por la evolución de la IA y su incidencia directa en la seguridad de las organizaciones.

UN DEBATE REGULATORIO QUE DEJA DE SER TEÓRICO

La discusión regulatoria dejó de ser abstracta y se volvió operativa. Durante 2026, la evaluación de la IA no solo se orientará a su capacidad de innovación, sino también a su impacto en derechos, seguridad y gobernanza.

La Artificial Intelligence Act introdujo un enfoque basado en el riesgo que establece:

- Obligaciones de transparencia y etiquetado de contenido sintético.
- Restricciones a usos de alto riesgo (biometría, manipulación conductual, infraestructura crítica).
- Deberes específicos para modelos de propósito general (GPAI).
- Aplicación escalonada hasta 2026.

La transición es clara: ya no basta con diseñar marcos legales; ahora es imprescindible implementarlos, supervisarlos y auditar su cumplimiento real.

Para las organizaciones, este escenario implica:

- Controles de integridad sobre información generada o procesada por IA.
- Mayor escrutinio de la cadena de proveedores tecnológicos.
- Políticas de respuesta a incidentes vinculados a IA.
- Intervención humana en decisiones críticas ("human in the loop") para mitigar riesgos de automatización opaca.

La regulación, en este contexto, no frena la innovación: redefinirá los estándares mínimos de confianza digital.

AMÉRICA LATINA: AVANCES ESTRATÉGICOS Y BRECHAS ESTRUCTURALES

- En la región, el nivel de preparación es heterogéneo. El Comisión Económica para América Latina y el Caribe (CEPAL), junto con el Centro Nacional de Inteligencia Artificial (CENIA), desarrolló el Índice Latinoamericano de Inteligencia Artificial (ILIA), que mide el nivel de preparación y adopción de la IA en 19 países, integrando dimensiones de factores habilitantes, I+D y gobernanza.

Su propósito es ofrecer un diagnóstico estratégico que permita a gobiernos y empresas entender dónde están y hacia dónde avanzar, fomentando competitividad e inversión responsable en el ecosistema de IA regional. Busca ser una herramienta para el diseño de regulaciones, estrategias y políticas nacionales de IA, alineadas con estándares internacionales y adaptadas a las necesidades locales.

De acuerdo con ILIA 2025, solo 8 de los 19 países analizados cuentan con estrategias o políticas públicas formales de IA: Argentina, Brasil, Chile, Colombia, Costa Rica, Perú, República Dominicana y Uruguay.

Este avance convive, de todas formas, con vacíos críticos en privacidad, gobernanza de datos y responsabilidad legal, que afectan la resiliencia de infraestructuras críticas y la confianza pública en sistemas basados en IA.

La ausencia de marcos robustos puede derivar en uso indebido de datos, sesgos algorítmicos y vulnerabilidades en sistemas críticos, afectando tanto la resiliencia de infraestructuras como la confianza pública.

Las estrategias nacionales permiten establecer principios éticos, definir responsabilidades legales y garantizar que la IA se utilice para impulsar el desarrollo económico sin comprometer la seguridad. Además, facilitan la cooperación internacional y la atracción de inversión tecnológica, factores clave para reducir la brecha digital en la región.

A pesar de que los países cuentan con algún plan, estrategia o política aún les hace falta abordar temas como ciberseguridad, privacidad de los datos que ingresen a los modelos de IA locales, la responsabilidad en la definición y utilización de los modelos/algoritmos, la gobernabilidad y soberanía de los datos.

Aquí es donde cuestiones relevantes sobre la regulación deberán de tratarse para brindar a cada uno de los ciudadanos de cada país una mayor seguridad, evitar sesgos y discriminaciones por los modelos de IA, principalmente:

- **Responsabilidad:** ¿Quién es responsable cuando un

sistema de IA causa daños? ¿Se tienen las competencias técnicas para revisar los modelos de IA?

- **Tratado de datos**: ¿Se tiene el consentimiento del usuario? ¿Se le notifica sobre la transparencia y explicabilidad de cómo serán usados sus datos?

- **Ser claros en dónde se guardarán los datos:** La recopilación y el análisis de grandes cantidades de datos para entrenar modelos de IA plantea importantes preocupaciones tales como ¿dónde se almacenarán los datos? (en servidores externos o propios).

- **Transparencia de los resultados que da la IA:** La IA debe ser rastreable y comprensible para cualquier tipo de público lo que origina una IA Explicable (XAI).

- **Evitar sesgos en los modelos de IA:** Los modelos de IA pueden perpetuar los sesgos presentes en los datos de entrenamiento, lo que puede llevar a decisiones injustas o discriminatorias.

- **Protección de algoritmos de IA frente a intenciones poco éticas:** Implementar una detección de anomalías en el entrenamiento de modelos, realizar monitoreos y evaluaciones continuas de sus algoritmos.

POR QUÉ LA REGULACIÓN IMPORTA: EL "TRIÁNGULO" DEL IMPACTO DE LA IA EN CIBERSEGURIDAD

El Foro Económico Mundial identifica tres vectores que conforman el nuevo equilibrio de la ciberseguridad impulsado por la IA. Este "triángulo" permite comprender de manera integral cómo se redistribuyen las capacidades ofensivas y defensivas, así como los riesgos emergentes para las organizaciones:

- **Expansión de la superficie de ataque y mayor impacto operativo**

La adopción de IA en procesos y cadenas de suministro introduce componentes altamente interdependientes —modelos, datos, prompts, agentes y pipelines de MLOps— que habilitan nuevos vectores de ataque. Estos incluyen envenenamiento de datos, manipulación de inferencias, evasión de modelos o compromiso de proveedores tecnológicos.

El impacto trasciende lo técnico: puede interrumpir procesos esenciales, degradar indicadores críticos del negocio y deteriorar la confianza del cliente.

- **Defensas potenciadas mediante IA**

La IA eleva las capacidades del ecosistema defensivo al habilitar detección basada en comportamiento, análisis masivo de telemetría y automatización coordinada de respuesta.

En entornos XDR y en nubes de seguridad, esto se traduce en menores tiempos de detección, mayor precisión y reducción de falsos positivos.

- **Escalamiento de amenazas impulsado por IA**

La IA también amplifica las capacidades ofensivas: desde spear phishing generado automáticamente hasta deepfakes de voz altamente verosímiles, pasando por herramientas que automatizan el descubrimiento de vulnerabilidades y la producción de malware adaptativo.
El resultado es un cibercrimen más rápido, más preciso y accesible incluso para actores con poca experiencia.

CONCLUSIONES: UN EQUILIBRIO URGENTE ENTRE INNOVACIÓN Y SEGURIDAD

La IA se consolida como un aliado fundamental para la defensa digital y, a la vez, como un vector de riesgo que exige gobernanza y regulación eficaces.
Aunque la región muestra avances —ocho países con estrategias formales de IA—, persisten brechas en privacidad, gobernanza de datos y responsabilidad legal, que deben abordarse con prioridad para proteger a la ciudadanía y fortalecer la resiliencia de los sistemas críticos.

La falta de marcos normativos sólidos abre la puerta a riesgos como sesgos algorítmicos, uso indebido de información y vulnerabilidades en infraestructuras críticas. Por ello, es fundamental que los gobiernos aceleren la creación de regulaciones claras, fomenten la transparencia y promuevan la cooperación regional. Solo así será posible equilibrar los beneficios de la IA con la protección de los ciudadanos y la resiliencia digital.

CONCLUSIÓN

El camino hacia un ecosistema digital más seguro en América Latina requiere un entendimiento profundo de las amenazas que atraviesan la región y de las capacidades que las organizaciones deben fortalecer para enfrentarlas. Los desafíos señalados a lo largo de este informe evidencian que la ciberseguridad ya no puede abordarse únicamente desde la reacción ante incidentes, sino desde una mirada estratégica que contemple la evolución tecnológica, los nuevos modelos de ataque y la creciente dependencia digital de los sectores público y privado.

Las tendencias analizadas reflejan un escenario en el que la automatización y la inteligencia artificial jugarán un rol determinante, tanto potenciando tácticas ofensivas como habilitando defensas más robustas. Sin embargo, esta dualidad exige redoblar los esfuerzos en materia de gobernanza, capacitación y adopción de prácticas preventivas que refuercen la resiliencia organizacional. La falta de visibilidad, la escasa implementación de controles esenciales y la insuficiencia regulatoria constituyen variables que deberán ser abordadas de manera urgente y sostenida.

Resulta claro que el fortalecimiento de las capacidades de ciberseguridad es un proceso continuo que demanda inversión, planificación y colaboración multisectorial. Las organizaciones que logren integrar estos elementos en su estrategia serán las mejor posicionadas para anticipar riesgos, proteger sus activos más críticos y adaptarse a un entorno donde las amenazas evolucionan con una velocidad sin precedentes.

Invitamos así a las empresas de la región a tomar este análisis como punto de partida para reflexionar sobre su propio nivel de preparación y avanzar hacia una cultura de seguridad más madura, proactiva y alineada con los desafíos que marcarán los próximos años.

CYBERSECURITY
EXPERTS ON YOUR SIDE