TENDENCIAS EN CIBERSEGURIDAD PARA EL 2025

Progress. Protected.

TABLA DE CONTENIDOS

INTRODUCCIÓN

Es fundamental identificar las tendencias que marcarán al mundo en materia de ciberseguridad en 2025, para la prevención, detección y una respuesta mucho más efectiva ante nuevas amenazas cibernéticas. "Conócete a ti mismo y conoce a tu enemigo, y en cien batallas nunca estarás en peligro ", reza uno de los principios clave de El arte de la guerra de Sun Tzu. Aplicándolo a la ciberseguridad, podríamos decir que "conócete a ti mismo" implica entender el cómo está protegida toda la infraestructura —nube y on premise—, identificar correctamente las vulnerabilidades aplicativas que existen intrínsecamente en cada una de ellas e implementar planes de contingencia que prioricen aquellos activos donde la información sea más crítica.

Año tras año, la información se ha transformado en un tesoro que todos los cibercriminales añoran tener en sus manos y pasó a convertirse en el nuevo oro del siglo XXI. "Conoce a tu enemigo", se traduce en poder entender y estudiar todas las tácticas, técnicas y procedimientos (TTPS) que los cibercriminales utilizan para hacerse dueños de esa información.

En el último *ESET Security Report 2024* hemos presentado los 12 datos sobre el estado de ciberseguridad de las empresas en América Latina. El dato más destacado del documento es que 1 de cada 5 organizaciones sufrieron al menos un incidente de seguridad, y los sectores más afectados fueron los organismos de gobierno, informática/tecnología y banca/finanzas. Por otro lado, el 62% de las organizaciones consideró que el presupuesto asignado a la ciberseguridad es insuficiente, a la vez que el 28% indicó que la ciberseguridad es un asunto de máxima preocupación.

Con este contexto, los especialistas del Laboratorio de Investigaciones de ESET Latinoamérica analizaron tres tendencias para tener en cuenta durante el 2025 que consideran que tendrán impacto destacado por haber mostrado en 2024 un continuo crecimiento y relevancia en la región, y que puede estimarse que seguirán prevaleciendo durante este año que empieza.

Para los encargados de la seguridad informática, cada inicio de año se vuelve un reto debido a que los activos tecnológicos poseen, generan y almacenan información cada vez más sensible de sus usuarios y clientes. Se hace necesario la generación o actualización de políticas y estrategias que permitan la accesibilidad, integridad y disponibilidad de esta información.

La ciberseguridad, aseguran los autores de este documento, deberá ser una prioridad estratégica para las altas direcciones de las empresas u organismos, donde el eje central debe ser una participación transversal de las áreas tecnológicas, operativas, administrativas y de gobernanza que identifiquen los riesgos cibernéticos a los que están expuestos en lo particular y lo general.

Una de las tendencias detectadas es el uso de la Inteligencia Artificial Generativa y las tecnologías emergentes, cuyo impacto irá más allá de solo automatizar tareas complejas y analizar grandes volúmenes de datos. Así como puede utilizarse para localizar tráfico malicioso en tiempo real para una respuesta más efectiva ante un ciberataque, también seguirá la tendencia hacia su uso maliciosos: crear campañas de phishing mucho más sofisticadas y convincentes dentro de la ingeniería social, en la sofisticación de las deepfakes —y su posible interacción con la realidad virtual—, sin pasar por alto el desarrollo de malware polimórfico capaz de evadir nuevos controles y tecnologías de seguridad.

Otra arista de este crecimiento exponencial de la Inteligencia Artificial Generativa y su capacidad para un uso malicioso trae aparejada la segunda tendencia que se destaca en este documento: los desafíos legales y éticos que surgen por la utilización de estas tecnologías.

A nivel mundial, y en particular en la región de América

Latina, las normativas que abarcan las problemáticas emergentes del empleo de la Inteligencia Artificial Generativa, resultan insuficientes frente a un panorama de desarrollo acelerado. Los marcos regulatorios desarrollados pueden quedar obsoletos o desactualizados si los avances normativos no van a su ritmo.
Por último, la tercera tendencia destacada por el Laboratorio de ESET es el impacto que el cibercrimen tienen en un sector que a veces no es tomado en cuenta en materia de ciberseguridad: los Sistemas de Control Industrial o también llamados Tecnologías Operativas (OT, por sus siglas en inglés). La digitalización y conectividad de estos sistemas los ha vuelto un blanco atractivo para los ciberataques.

Estos sistemas informáticos, que incluyen dispositivos, son utilizados para controlar procesos industriales y físicos en diversos sectores, como la energía, manufactura, agua y gas, entre los principales. A su vez, gestionan equipos como PLC (Controladores Lógicos Programables), SCADA (Sistemas de Control Supervisorio y Adquisición de Datos) siendo sus funciones principales la automatización de procesos, el monitoreo-análisis de operaciones y la gestión de información en ambientes productivos.

Existen eventos históricos donde se han visto códigos maliciosos que tienen como objetivo vulnerar estos sistemas. Entre los que podemos destacar es el nombrado "Aurora Generator Test", una prueba del gobierno de los Estados Unidos que demostró en 2007, por primera vez, que un ciberataque podía causar daños físicos a un generador de energía. Otros ejemplos son los malware BlackEnergy, Industroyer o Industroyer 2, que se utilizaron en distintos momentos en ataques a la red eléctrica de Ucrania.
Conforme la tecnología avanza, la exposición de ataque también incrementa, por eso es importante darle un enfoque de seguridad basado en la confianza cero (Zero Trust, en inglés). En otras palabras, ningún activo tecnológico o actor puede ser confiable por defecto y, por lo tanto, debe de existir una verificación continua de su identidad, para que, en caso de no lograr comprobar su identidad, se tomen las medidas correspondientes, reduciendo esa superficie de ataque.

No solo es cuestión de implementar tecnologías de última generación o enfoques para salvaguardar la información de los usuarios, sino también es fundamental hacer conciencia y capacitar a todos los niveles de una organización sobre las buenas prácticas que deben aplicarse, es decir, que le brinde al usuario las herramientas que le permitan identificar posibles riesgos cibernéticos para empoderarlos y así reducir la posibilidad de un ciberataque.

La ciberseguridad debe de ser una tarea transversal para todas las áreas dentro de una organización, pues estar conscientes de estas tendencias, les permitirá sumar o actualizar políticas y tecnologías para enfrentar los desafíos emergentes del 2025.

1

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL GENERATIVA EN LA CIBERSEGURIDAD

Mario Micucci
Security Researcher
ESET Latinoamérica

La inteligencia artificial generativa, representada por modelos avanzados como ChatGPT y DALL-E, han revolucionado la forma en que creamos, consumimos y entendemos la información en estos días. Esta tecnología, capaz de generar textos, imágenes, música y código de manera autónoma, promete transformar múltiples industrias y sectores. Y en ciberseguridad, así como aporta nuevas herramientas para detectar, prevenir y responder a amenazas, también amplía las capacidades de los actores maliciosos.

En un entorno donde los ciberataques son cada vez más sofisticados, la inteligencia artificial generativa ofrece soluciones que permiten automatizar tareas complejas, como el análisis de grandes volúmenes de datos y la simulación de escenarios de ataque. Y también esta misma tecnología puede ser utilizada para crear campañas de phishing más convincentes, sesgar modelos de IA, desarrollar malware polimórfico y amplificar el alcance de las amenazas tradicionales.

Para los gerentes de ciberseguridad, entender cómo esta tecnología está transformando las dinámicas de defensa y ataque es fundamental. La clave estará en adoptar un enfoque equilibrado, aprovechando las oportunidades que la IA generativa ofrece, y establecer salvaguardas sólidas para proteger a las empresas y a los usuarios frente a sus posibles abusos.

LA IA GENERATIVA AL SERVICIO DEL CIBERCRIMEN

Si bien hemos visto las bondades de la inteligencia artificial generativa al servicio de la ciberseguridad, es importante destacar como una tendencia para 2025 su uso malicioso que estimamos se intensificará en las siguientes áreas:

SPEAR-PHISHING AVANZADO

Esencialmente, hablamos de la creación automatizada de correos electrónicos y mensajes personalizados basados en análisis de datos públicos y privados, que aumentan la efectividad de los ataques. La IA generativa puede analizar grandes cantidades de datos públicos y privados para crear mensajes altamente personalizados y creíbles.

Herramientas como ChatGPT o similares pueden generar mensajes que imiten perfectamente el tono y estilo de comunicación de una persona o entidad. Por ejemplo, al obtener datos de redes sociales, se pueden generar correos dirigidos que mencionen eventos recientes o temas sensibles para la víctima.

Estos mensajes son difíciles de distinguir de los reales, incrementando la probabilidad de que las víctimas hagan clic en enlaces maliciosos o revelen información confidencial.

FALSIFICACIÓN DE IDENTIDADES

La generación de deepfakes para suplantar a individuos en *videollamadas o mensajes de voz utilizados para fraudes o extorsión* se muestra en alza. La generación de videos y audios falsos realistas (deepfakes) sin dudas seguirá siendo utilizada para engañar a individuos y organizaciones.

Con suficientes datos de audio o video de una persona (por ejemplo, obtenidos de redes sociales o conferencias públicas), la IA generativa puede crear contenido falso que reproduzca su voz o apariencia. Esto puede utilizarse para convencer a empleados de transferir fondos o acceder a sistemas críticos.

Las estafas que antes se realizaban por texto ahora tendrán un nivel de realismo que dificultará la detección incluso para usuarios capacitados.

PROPAGACIÓN DE DESINFORMACIÓN:

Este año hemos visto el *uso de la IA generativa para diversas campañas* con el objetivo de desinformar o sesgar la opinión pública. Hoy el uso masivo de texto, imágenes y videos generados por IA para manipular la opinión pública se muestra como una tendencia, sobrecargando las capacidades de verificación de hechos. La IA generativa permite crear y distribuir contenido falso de manera masiva y altamente convincente.

Modelos de IA pueden generar artículos, imágenes y videos que parecen auténticos. Esto incluye falsificar declaraciones de figuras públicas, crear noticias ficticias o manipular evidencias visuales para respaldar narrativas falsas. Su impacto es claro: socava la confianza pública en las instituciones, afecta procesos democráticos y fomenta la polarización social. En América Latina, este tema *genera preocupación*.

CREACIÓN DE MALWARE:

- Cada vez se puede observar más la generación asistida de código malicioso más sofisticado y ofuscado, aprovechando modelos avanzados de IA para evadir detecciones. La IA generativa puede facilitar la escritura de código malicioso más sofisticado y difícil de detectar.

- Modelos como Codex pueden sugerir estructuras de código optimizadas para evadir mecanismos de detección, incluyendo técnicas avanzadas de ofuscación o polimorfismo. Además, la IA puede automatizar pruebas para identificar puntos débiles en sistemas.

- Aumenta la velocidad y la sofisticación del desarrollo de malware, reduciendo las barreras técnicas para los ciberdelincuentes menos experimentados.

AUTOMATIZACIÓN DE ATAQUES:

Si hay algo que cada vez caracteriza más al cibercrimen

es la automatización de sus tareas, mediante el uso de IA generativa se pueden por ejemplo realizar pruebas masivas en infraestructuras, buscando vulnerabilidades explotables. La IA generativa puede automatizar procesos en ciberataques, desde el reconocimiento hasta la explotación de vulnerabilidades.

Recientemente OpenAI, la compañía detrás de ChatGPT, *emitió un informe* en que detalla cómo se utilizaron sus modelos de IA para realizar tareas de fases intermedias en los ciberataques. En el mismo informe, la empresa identifica que distintos grupos APT (Amenazas Persistentes Avanzadas) han utilizado la tecnología para, por ejemplo, el debugging de código malicioso, la investigación de vulnerabilidades críticas, el perfeccionamiento de phishing, generación de imágenes y comentarios falsos, entre otras.

Además, el uso de bots impulsados por IA puede utilizarse para escanear continuamente redes y sistemas, buscando configuraciones incorrectas, puertos abiertos o software desactualizado. Una vez identificada una vulnerabilidad, pueden generar scripts de explotación específicos al instante.

Incrementa la escala de los ataques, permitiendo a los ciberdelincuentes dirigir ataques simultáneamente contra múltiples objetivos con un costo marginal bajo.

ÁREAS DE LA CIBERSEGURIDAD AFECTADAS POR LA IA GENERATIVA

Es un hecho que la llegada de la inteligencia artificial generativa está marcando un antes y un después en la ciberseguridad, impactando múltiples áreas clave de conocimiento y operación. Analicemos algunas de las más relevantes:

1. Defensa Cibernética Avanzada

Los modelos de IA generativa están revolucionando cómo las organizaciones identifican y mitigan amenazas. Gracias a su capacidad para analizar patrones de comportamiento en tiempo real, estas herramientas pueden:

- Detectar ataques antes de que causen daño significativo, identificando anomalías en grandes volúmenes de datos de red.
- Proponer respuestas automatizadas a incidentes, como bloqueos de IP sospechosas o ajustes dinámicos en las configuraciones de firewall.

Por ejemplo, un sistema basado en IA generativa podría analizar tráfico en tiempo real, identificar un ataque de DDoS emergente y desplegar contramedidas en cuestión de segundos.

2. Simulación de Amenazas

La IA generativa facilita la creación de escenarios hiperrealistas para pruebas de ciberseguridad, lo que permite a las organizaciones:

- Simular ciberataques avanzados para evaluar la resiliencia de sus sistemas.
- Generar amenazas hipotéticas basadas en tácticas emergentes de actores maliciosos, ayudando a diseñar defensas preventivas.

Un ejemplo es el uso de IA para generar correos electrónicos de phishing simulados que se ajustan al perfil de un empleado, entrenando a los equipos internos a reconocer señales de alerta.

3. Desarrollo de Capacidades Humanas

El entrenamiento en ciberseguridad se está transformando gracias a la IA generativa, permitiendo:

- Crear contenido educativo personalizado para cada nivel de usuario.
- Diseñar escenarios de entrenamiento dinámicos, como simulaciones de ataques dirigidos a perfiles específicos.

Por ejemplo, las organizaciones más vanguardistas están comenzando a utilizar IA generativa para adaptar sesiones de capacitación sobre phishing según el rol de los empleados, maximizando el impacto y minimizando las brechas de conocimiento.

4. Automatización de Respuestas Forenses

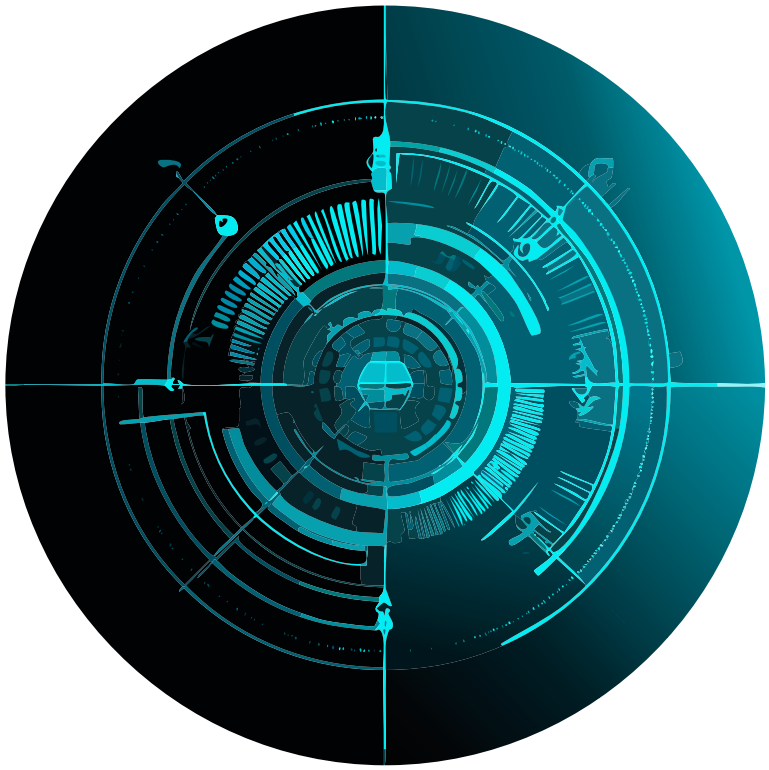
En incidentes de seguridad, el tiempo es crucial. Y la IA generativa puede jugar un rol fundamental para:

- Organizar y analizar grandes volúmenes de logs en busca de patrones que identifiquen la causa raíz de un ataque.
- Generar informes detallados con posibles soluciones y recomendaciones específicas para cada escenario.

Esto no solo acelera la respuesta a incidentes, sino que también reduce la carga operativa de los equipos forenses, permitiéndoles centrarse en tareas críticas.

El observar los detalles sobre estas áreas muestran cómo la IA generativa no solo está ampliando las capacidades defensivas, sino también redefiniendo la manera en que las organizaciones comienzan a pensar y actuar frente a los aspectos de la ciberseguridad. Sin embargo, no podemos dejar de destacar que este potencial viene acompañado de desafíos significativos.

Si bien el panorama de usar IA como herramienta defensiva es prometedor, no podemos dejar de considerar que también la están utilizando los adversarios, y que sobre todo su eficiencia depende de la calidad de los datos con las que esta sea entrenada y la robustez de los algoritmos utilizados. En esta línea surgen varios interrogantes que serán necesarios responder como, ¿con qué calidad de datos están y van a hacer entrenados los sistemas de IA?, ¿quién y cómo se han supervisado y seleccionado esos datos?, ¿qué tipo de algoritmos están y serán utilizados para entrenar a estos sistemas?, ¿bajo qué criterios estos sistemas toman y podrán tomar decisiones?



2

LOS DESAFÍOS LEGALES Y ÉTICOS DEL AVANCE DE LA INTELIGENCIA ARTIFICIAL GENERATIVA

Fabiana Ramírez Cuenca
Security Researcher
ESET Latinoamérica

Frente al crecimiento que se ha experimentado en la inteligencia artificial generativa y su potencial uso malicioso, aparecen desafíos legales y éticos que en su mayoría aún no han sido eficientemente abordados. ¿Quién es el responsable por los actos de la inteligencia artificial? ¿Qué límites debería imponerse a su desarrollo? ¿Qué organismo es competente para juzgarlo?

En la actualidad existen muy pocas normas a nivel internacional que aborden las problemáticas emergentes del uso de la IA y aquellas que existen muchas veces resultan insuficientes frente a un panorama de desarrollo acelerado de esta tecnología.

De todas formas, durante este año es probable que la tendencia principal en estas cuestiones sea un mayor escrutinio en los algoritmos y modelos de IA para garantizar transparencia y explicabilidad y normativas que se orienten a la protección de datos para garantizar la privacidad en el uso de la IA.

Veremos la búsqueda de soluciones para los daños generados por la IA y la promoción, desde lo regulatorio, de la ética en la utilización y desarrollo de esta tecnología. También seguirán los avances en regulaciones sobre ciberseguridad aplicadas a la temática y en materia de cooperación internacional.

La inteligencia artificial en todos sus tipos nos ha traído una gran cantidad de beneficios. Hoy en día contamos con diversos algoritmos de automatización de procesos, aplicables a distintas áreas. También vemos la IA en la vida cotidiana, enfocada en usuarios hogareños pudiendo mencionar como ejemplo a los asistentes de voz y a las IA capaces de procesar lenguaje natural entre las que podemos destacar a ChatGPT, Gemini, Copilot y Meta AI, que son quizás las implementaciones más conocidas, pero no las únicas. Y esto no es todo, sino que hemos visto un amplio crecimiento del uso de la IA Generativa en todas sus formas, así como nuevas implementaciones en el área de la salud para mejorar los diagnósticos y hasta se está experimentando en la cirugía. Estos se reiteran, son solo algunos de los muchos usos de la IA en la actualidad.

Sin embargo, los algoritmos están al alcance de todos, existiendo una gran cantidad de fuentes abiertas de las cuales se puede obtenerlos, personalizarlos y darles además usos menos éticos entre los que podemos destacar la creación o perfeccionamiento de códigos maliciosos, generación de deepfakes y fakenews por nombrar los más notorios.

Podemos destacar que los algoritmos de IA no son maliciosos como tal, sino que esto está dado por el uso que le den los humanos. Esta tecnología se ha creado en principio para servir a la humanidad, pero hay quienes la implementan con fines ilícitos, lo que demuestra la potencialidad de la IA para causar daño, muchas veces por su uso intencional y otras solo por un desarrollo inseguro o descuidado de los algoritmos.

DESAFÍOS EN LA IMPLEMENTACIÓN DE LA IA

Si nos paramos frente a la IA actual y observamos sus usos, está claro el porqué de su implementación, que no es menos que facilitar a los humanos la ejecución de diversas tareas, en tanto los algoritmos son capaces de llevar adelante estas en forma más rápida y muchas veces hasta más precisas.
Pero al momento del desarrollo de los algoritmos y posterior uso, en principio, no se ha tenido en cuenta cómo podría afectar esto a diversas cuestiones vinculadas a los derechos humanos. Vale aclarar que lo mismo ha pasado con la mayoría de las tecnologías al inicio de su implementación y no es una característica propia de la IA.

En efecto, podemos mencionar algunos desafíos relacionados con esta cuestión:

- **Privacidad de datos:**

Los modelos de IA son entrenados con grandes cantidades de datos, lo que de entrada plantea cuestiones alrededor de cómo se recopilan, almacenan y utilizan estos datos, especialmente cuando se trata de información personal. Al respecto, a nivel legal, los usuarios deben consentir la recopilación y tratamiento de datos, pero para que el consentimiento sea válido debe ser informado (esto significa que el usuario realmente comprenda toda la cuestión) y es aquí donde cabe preguntarse si los usuarios realmente comprenden como se utilizarán los datos o para qué. La IA, además, puede utilizarse para rastrear, perfilar y monitorear a las personas en distintos aspectos de su vida, lo que plantea preocupaciones sobre la privacidad y hasta la libertad individual.

- **Calidad de los datos:**

Los datos con los que se entrenan los modelos de IA pueden contener sesgos, lo que puede llevar a resultados discriminatorios o injustos. En efecto, la calidad de los datos puede variar y afectar la precisión y fiabilidad de los resultados obtenidos por los modelos de IA. La calidad implica que los datos cumplan ciertas características como la precisión, integridad, consistencia, relevancia, actualidad, accesibilidad y veracidad.

- **Propiedad intelectual:**

Al ser los modelos capaces de generar contenido de todo tipo, característica que, por supuesto hacen a partir de los datos con los que fueron entrenados, surgen varias cuestiones como quién resulta propietario de obras generadas (si la empresa desarrolladora o el usuario que solicita la generación). Frente a esto, también cabe preguntarse cómo se aplican las leyes a los contenidos generados con IA y de qué forma podría detectarse un plagio, al menos parcial.

- **Transparencia:**

Muchos algoritmos de IA, como por ejemplo los de Deeplearning, llegan a puntos de complejidad que los convierte en difíciles de comprender incluso para sus desarrolladores, cosa que dificulta la evaluación de su funcionamiento. Esto puede traer aparejado que algunas veces, frente a determinados resultados, no se pueda explicar exactamente como la IA ha concluido los mismos. Es importante desarrollar modelos que sean capaces de explicar cómo llegan a sus conclusiones, en tanto la información es un derecho de la ciudadanía y conocer el hilo de trabajo del modelo permitirá ajustarlo de ser necesario.

- **Manipulación de la información:**

La IA y su gran capacidad generativa puede utilizarse para crear contenido falso, como videos o audios, así como ampliar la difusión de fakenews. Todo esto muchas veces implica que sea difícil diferenciar entre lo falso y lo real, pudiendo aprovecharse la tecnología para desinformar y hasta manipular la opinión de la ciudadanía.

- **Uso vinculado a las armas:**

Se sabe que la IA también viene siendo utilizada en el ámbito militar y se experimenta con sistemas de armas autónomos que eventualmente podrían ocasionar daños a la humanidad si no se establecen límites.

- **Reemplazo laboral:**

La IA permite automatizar muchas tareas, lo que podría conducir a una pérdida de determinados empleos, por reemplazo. Sin embargo, se considera que el humano deberá aprender a trabajar con esta tecnología, en tanto las ofertas de trabajo variarán y no se reducirán. La automatización potencialmente puede agrandar la desigualdad económica, ya que los beneficios de la IA se concentrarían en un pequeño grupo de personas y también la profesionalización necesaria para trabajar con la tecnología sería más accesible a sectores con mayores ingresos económicos.

- **Seguridad en la implementación y desarrollo:**
Como todo sistema, los modelos de IA pueden ser vulnerables a ataques cibernéticos, lo que podría tener consecuencias graves según el caso. La IA al utilizarse también en sistemas de gran escala (energía, transporte, etc.) puede tener impactos amplios en caso de ser atacada.

- **Alucinaciones y derecho a la realidad:**
Los modelos de IA pueden generar respuestas incorrectas o sin sentido a pesar de ser entrenadas de la mejor manera, con lo cual es importante la consciencia de esto y regular la confianza en los algoritmos. Esto va de la mano con un planteo interesante referido al "*Derecho a la Realidad*" que es una nueva propuesta doctrinaria que dice que, frente a toda esta tecnología, el humano tiene derecho a acceder y saber la verdad y por tanto se deben reducir al máximo las alucinaciones, fakenews, deepfakes entre otras falsedades a las que puede arribar una IA.

- **Sesgos:**
Las conclusiones de la IA pueden perpetuar sesgos presentes en los datos con los que son entrenados, dando como resultado decisiones discriminatorias en diversas áreas como la contratación laboral, legal, entre otras.

La IA puede utilizarse para desarrollar o perfeccionar ataques cibernéticos, como por ejemplo para análisis o generación de código malicioso.

DESAFÍOS REGULATORIOS

Frente al panorama que nos plantea la implementación de IA, a nivel legal, surgen varios interrogantes que la mayoría de las veces aún quedan sin responder.

- **¿Quién es competente para resolver cuestiones sobre IA?**
La competencia para resolver cuestiones sobre IA es un tema complejo que aún se encuentra en evolución, ya que para establecerse debe tenerse en cuenta varias disciplinas, no solo el derecho sino también la tecnología, la ética, entre otras. Es difícil determinar en qué territorio se juzgaría por daños generados con IA, o que juzgado sería competente, por ejemplo. Es posible que se deba acordar esto a nivel internacional, en tanto la implementación de la IA va más allá de los límites geográficos.

¿Quién es responsable por la IA?

Si el uso de la IA recae en daños cabe preguntarse quién es responsable frente a esos daños y es esto quizás una de las temáticas más discutidas de la actualidad, dado que hay varios actores a quienes se podría atribuir la responsabilidad. Por un lado, los desarrolladores de la IA que deben hacerlo en forma segura a fin de que el modelo sea confiable, luego tenemos a quienes comercian con el modelo (empresas) que deben supervisar el producto a fin de disminuir sus riesgos. Y también tenemos al usuario final, que debe utilizar los modelos en forma responsable cumpliendo con términos y condiciones.

Según el caso, la responsabilidad podría ser compartida. Aunque como venimos mencionando, aun la legislación a nivel internacional no ha resuelto este tema.

¿La IA ejecuta hechos o actos?

Cuando un humano genera un daño, por ejemplo, este es causado por un acto realizado por el humano en cuestión. Estos actos son hechos, pero que son realizados con discernimiento, intención y libertad y su consecuencia en primeras instancias en responsabilidad del actor.

Pero si pensamos en consecuencias causadas por la IA, siendo la IA una tecnología carente de razonamiento y emocionalidad, podríamos asumir que no realiza actos, sino que solamente genera hechos. Y frente a esto, volvemos a la pregunta anterior.

AVANCES A NIVEL REGULATORIO

- Con la finalidad de poner orden a todo lo atinente a la IA algunos estados han estado trabajando en regulaciones internas y a nivel internacional ha habido pequeños avances.

Podemos destacar:

- El *Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de derecho*, que durante 2024 fue abierto a firma y puede considerarse como el primer tratado internacional vinculante (obligatorio). Entre los firmantes están

Andorra, Georgia, Islandia, Noruega, la República de Moldavia, San Marino, Reino Unido, así como Israel, Estados Unidos de América y la Unión Europea.

- En 2021 pudimos ver las *Recomendaciones de la UNESCO*, que fueron un marco ético, aunque no vinculante.

- Durante el 2023, se destaca el *Acta de IA de la Unión Europea* (quizás la norma más completa de la actualidad, con un enfoque basado en la clasificación de la IA según riesgos), la Política Nacional de IA de los Estados Unidos y la orden ejecutiva del presidente Biden y más recientemente el tratamiento por parte de los Estados Unidos de un Proyecto de Ley sobre IA (IA Blueprint).

- A nivel LATAM no ha habido grandes avances durante el 2024 aunque la mayoría de los países cuentan al menos con decretos, salvo el caso de *Perú que cuenta con una ley*.

- El Parlatino (Parlamento Latinoamericano y Caribeño) en 2017 había creado una *ley modelo para los países miembro* con el objeto de promover la regulación de la Inteligencia Artificial. Esta ley modelo propone principios éticos y mecanismos de gobernanza y protección de datos.

- Podemos destacar que la regulación de la IA en forma individual resultaría insuficiente, en tanto la cuestión es además atravesada por la normativa de protección de datos y de ciberseguridad.

3

TECNOLOGÍAS OPERATIVAS EN LA MIRA

Martina López
Security Researcher
ESET Latinoamérica

Históricamente, los sistemas industriales fueron diseñados para operar de forma analógica y aislada, pero luego fueron introduciendo tecnologías con un enfoque centrado en garantizar la confiabilidad y disponibilidad, más que en la seguridad. Estas implementaciones tecnológicas surgen de la introducción de cualidades de la tecnología de la información a sistemas físicos ya existentes, con el objetivo de reemplazar mecanismos físicos secundarios, así como introducir nuevas características preservando el ciclo de vida industrial del mismo, sin hacerlo más corto, similar a los sistemas 100% informáticos.

Como contracara, esta integración creciente y entrelazada con la digitalización y el ahora auge del Internet Industrial de las Cosas (IIoT) da espacio a la sobreexposición de estos sistemas complejos a amenazas maliciosas, diseñadas a medida y con variadas motivaciones.

Los incidentes dirigidos a OT son cada vez más frecuentes, viendo involucradas amenazas desde el recordado *Stuxnet*, pasando por *NotPetya* hasta *Triton*. Estos incidentes han demostrado que comprometer sistemas OT no solo afecta a organismos o instituciones, sino que puede desencadenar crisis nacionales con impactos económicos, sociales y hasta ambientales.

¿QUÉ ES LA TECNOLOGÍA OPERATIVA (OT)?

Tecnología operativa (OT, por sus siglas en inglés) es un término que engloba una serie de sistemas y dispositivos programables que interactúan con entornos físicos en contextos industriales. Esta interacción puede ser en formato de monitoreo o control de procesos o eventos, teniendo un impacto palpable en estos sistemas: Controlar una temperatura, dejar fluir componentes químicos, monitorear cargas de otros sistemas.

OT abarca los sistemas que controlan y monitorean procesos físicos en industrias críticas como la energía, la manufactura, el transporte y el suministro de agua. Estos sistemas son el corazón de las infraestructuras que sustentan la vida moderna, desde la red eléctrica hasta las plantas de tratamiento de agua y los sistemas de transporte público.

Entre los sistemas OT más comunes encontramos el Internet de las Cosas Industrial (IIOT), los sistemas de Control Supervisor y Adquisición de Datos (SCADA), los Controladores Programables Lógicos (PLC) y los Sistemas de Control Distribuido (DCS). Estos conforman, junto a sistemas de control manual y operarios, una topología de red compleja cuya implementación presenta pormenores que quedan fuera de este documento.

ADVERSARIOS A LA TECNOLOGÍA OPERATIVA

En el ámbito de la tecnología operativa, las consecuencias de un ciberataque no se limitan a pérdidas económicas o a la exposición de información confidencial. Aquí, como en muchos casos hablamos de infraestructuras críticas, los ataques tienen el potencial de generar interrupciones significativas en servicios esenciales, como el suministro de energía, el transporte o la producción industrial, e incluso de poner en riesgo la seguridad física de personas e infraestructuras.

Estos ataques trascienden lo digital, convirtiéndose en amenazas al entorno físico y, en última instancia, a la estabilidad social y económica. Y es allí donde se encuentra el atractivo para los actores maliciosos, con motivaciones tan diversas como sí mismos.

En la *guía de ciberseguridad de OT publicada por el NIST* se delinean cuatro categorías de actores que representan un riesgo para esta, dependiendo del origen de los actores mismos. Estas son ambientales (como las catástrofes naturales), estructurales (fallos de hardware, software o redes), accidentales (por acciones erróneas tomadas por un individuo) o adversariales.

Los actores "adversarios" son lo que catalogamos como atacantes, en una similitud con el abordaje de la ciberseguridad corporativa, pero con componentes adicionales. Se trata de cualquier individuo, grupo o estado que busque perjudicar a la compañía dueña de la infraestructura, explotando su (adecuada o excesiva) dependencia en sistemas tecnológicos.

Por su gran impacto, este ciberataque es elegido por perpetradores cuyas motivaciones se centran en la destrucción o alteración del funcionamiento de los sistemas. Un caso ampliamente recordado de esto es *Industroyer*, un código malicioso modular diseñado para afectar este tipo de infraestructuras. Puntualmente, esta amenaza usa cuatro componentes maliciosos (payloads), que están diseñados para obtener el control directo de interruptores y disyuntores en una subestación de distribución de electricidad mediante protocolos de comunicación específicos de OT. Con este control, el código malicioso pudo hacer uso de una de sus funcionalidades: la denegación de servicio, afectando a una planta de energía ucraniana.

Sin embargo, es vital no dejar de lado a ciberatacantes que estén detrás de una ganancia económica, ya sea como único objetivo o uno entre múltiples. De hecho, ya hemos sido testigos de este tipo de ciberataques, puntualmente aquellos que utilizan al ransomware como amenaza principal. Así sucedió el incidente hacia Colonial Pipeline en 2021, un importante oleoducto de combustible en Estados Unidos que vio irrumpida su actividad por un ciberataque atribuido al grupo DarkSide. Si bien los pormenores de lo ocurrido no salieron a la luz, sí sabemos que el atacante desplegó una amenaza de este tipo vía una cuenta de un servicio de VPN comprometida, para luego exigir un rescate.

PLANTEANDO ESTRATEGIAS DE CIBERSEGURIDAD

La ciberseguridad en tecnologías operativas despierta preocupaciones tanto en entidades gubernamentales como en sectores privados. Es entonces que surge la necesidad (o, al menos, el interés) de incorporar una estrategia de ciberseguridad acorde al riesgo de un posible incidente. Y, de hecho, las estrategias dirigidas a proteger la tecnología operativa suelen dedicar secciones enteras a la evaluación y manejo del riesgo: Aquí no solo intervienen pérdidas económicas por inactividad o consecuencias legales, sino también impacto en el medioambiente o la población general.

Los abordajes sugeridos por diversos veedores de la ciberseguridad incluyen una protección multinivel, considerando así todos los elementos involucrados en el ciclo de vida de la tecnología operativa: Hardware, software, redes, accesos físicos y, por supuesto, los operarios. En esta línea, agencias de ciberseguridad de diversos países publicaron en 2025 una *guía para responsables de Tecnologías Operativas* con consideraciones de seguridad a la hora de elegir productos tecnológicos para sus sistemas. Por último, también existen equivalencias aplicables de modelos de la ciberseguridad corporativa, como el Zero Trust, que pueden ser considerados para sistemas industriales.

Sin embargo, y a pesar del gran desarrollo en Latinoamérica de las industrias que más utilizan OT, este tipo de modelos sigue siendo un plan a futuro. Ya sea por falta de interés político, presupuesto, simple desconocimiento o una sensación de lejanía frente a estos incidentes (contrario a otras regiones del mundo), todavía hay un gran camino hacia la implementación de estas medidas de seguridad.

Lo cierto es que estos ataques se dan con cada vez más frecuencia, llegando a ser testigos de al menos un ataque de gran impacto por año. Y, si bien con un impacto variable y en algunos casos menor que en otras partes del mundo, Latinoamérica no es ajena a ello: Desde proveedores de red, pasando por compañías de suministro eléctrico y hasta aquellas dedicadas a la minería.

El progreso en esta temática en la región no es nulo. De hecho, varios gobiernos ya lo han incluido en sus planes de desarrollo de la ciberseguridad para años venideros, y *el chileno realizó en noviembre un simulacro de ataque*.

Los próximos años serán determinantes para evaluar si las medidas actuales son suficientes o si enfrentaremos una constante carrera entre la protección y los ciberataques en el ámbito de OT. Lo que es claro es que esta temática seguirá siendo clave en la agenda de ciberseguridad global y regional, marcando desafíos que nos seguirán acompañando en el futuro.

CONCLUSIÓN

A lo largo de este informe se desarrollaron tres tendencias que pueden marcar el 2025, desde la que involucra a la inteligencia artificial generativa y sus desafíos tanto en ciberseguridad como en lo normativo y ético, hasta los sistemas informáticos que son utilizados para controlar procesos industriales y físicos en diversos sectores, los llamados Sistemas de Control Industrial o también llamados Tecnologías Operativas (OT, por sus siglas en inglés). Es importante considerar cada una de ellas para este año porque, ya que las amenazas cibernéticas se encuentran en constante evolución, y buscan activamente la manera de evadir nuevas tecnologías o controles de seguridad.

A pesar de que la Inteligencia Artificial sigue siendo una tendencia durante y pospandemia, como toda nueva tecnología existen dos caras de la moneda. Por un lado, su impacto ha generado nuevas capacidades defensivas, redefiniendo la manera en que las organizaciones comienzan a pensar y actuar frente a los aspectos de la ciberseguridad. Por el otro, surgen varias interrogantes: ¿con qué calidad de datos están y van a hacer entrenados los modelos de Inteligencia Artificial?, ¿quién y cómo se han supervisado y seleccionado esos datos?, ¿existen medidas que permitan a los algoritmos la detección de sesgos que permitan la imparcialidad para identificar y abordar patrones discriminatorios de los datos?, ¿qué tipo de algoritmos son los más aptos para entrenar a estos sistemas?, ¿bajo qué criterios estos sistemas toman y podrán tomar decisiones?

Lo anterior podría dejar lagunas en las futuras leyes que pueden ser aprovechadas por los ciberdelincuentes para adquirir y entrenar a sus propios modelos de Inteligencia Artificial o en su defecto utilizar sistemas que no cumplan con las normativas para generar códigos maliciosos más sofisticados además de ataques de ingeniería social mucho más convincentes (deepfakes y la interacción con la realidad virtual).

¿Qué pasaría si la red eléctrica de una ciudad se viera comprometida por un ciberataque? La historia nos ha demostrado que esto es posible, las consecuencias no solo abarcarían lo monetario y los tecnológicos, sino que pondrían en peligro la vida de ciento de personas.

Cualquier activo en el ciberespacio puede ser vulnerado y es por ello que las organizaciones deben de implementar políticas y controles de seguridad que permitan resguardar el activo que hoy en día es lo más valioso que poseen: la información. Sin dejar a un lado que la capacitación constante en ciberseguridad para todo nivel del organigrama es fundamental para que los ciberataques se vean reducidos considerablemente. El eslabón más susceptible dentro de un sistema informático y por donde la mayoría de los ciberataques son exitosos se deben al usuario final.

La comprensión de las amenazas previstas para 2025 puede ayudar a las organizaciones a anticiparse a posibles actores emergentes, proporcionando una base sólida para definir o actualizar las políticas de seguridad en toda su estructura. Adoptar el modelo de confianza cero (Zero Trust) permitirá garantizar la protección del entorno digital y fomentar un progreso constante.

Esperamos que este informe ayude a comprender mejor una parte del panorama que se avecina, promoviendo así la colaboración para fortalecer las defensas digitales, prever las amenazas emergentes y proteger el patrimonio digital en un entorno cada vez más complejo y sofisticado.

CYBERSECURITY
EXPERTS ON YOUR SIDE