ESTRATEGIAS DE PROTECCIÓN

# LA IA ESTÁ REFORZANDO A LA CIBERDELINCUENCIA

Usar chatbots públicos y otras herramientas fruto de la inteligencia artificial generativa ahora deben considerarse al proteger a los clientes

En México y en la región las empresas que optan por utilizar los GPT existentes tienden a ser más susceptibles a daños o ataques a sus datos corporativos.

**CHARBEL CHALALA**
VICEPRESIDENTE DE VENTAS PARA LATAM

**POR PAUL LARA**
*paul.lara@gimm.com.mx*

El panorama de ciberseguridad en la región, especialmente en países clave como México y Brasil, es prioritario, "pues el simplificar la protección de los datos en el lugar de trabajo nunca ha sido tarea sencilla", afirman especialistas de Forcepoint.

Charbel Chalala, quien suma esfuerzos en la compañía de ciberseguridad como vicepresidente de Ventas para Latam, siendo responsable por toda la región, pero principalmente por las operaciones de Brasil y México, afirma que el último año fue desafiante.

"La evolución de las herramientas tecnológicas, y su consiguiente uso por parte de los delincuentes, ha hecho que haya aún más factores a considerar a la hora de desarrollar estrategias de protección de datos. Tanto para las pequeñas como para los grandes corporativos, es fundamental adoptar una política de Zero Trust o Cero Confianza", explica.

El uso de herramientas privadas de IA parece ser más seguro, pero muchas organizaciones dependen de soluciones públicas, como ChatGPT y esto implica que los datos ya no son propiedad exclusiva de la empresa, lo que enfatiza aún más la necesidad de centrarse en prevenir la exposición de información sensible. "Es por ello por lo que el objetivo de incorporar la IA debe centrarse en evitar la introducción inadecuada de información sensible en el gran desconocido de la IA generativa pública".

Para Chalala, en México y en la región las empresas que optan por utilizar los GPT existentes tienden a ser más susceptibles a daños o ataques a sus datos corporativos. "Por otro lado, las instituciones que opten por desarrollar su propio GPT tendrán aún más opciones que considerar. Las políticas corporativas y de seguridad existentes a menudo cubrirán el uso de datos cuando se implementen internamente los chatbots de IA personalizados", afirmó.

**EL DATO**

**La herramienta**

**GenAI es una solución integral de seguridad que ofrece visibilidad, control y protección de datos basada en riesgos en plataformas de IA generativa.**

Luiz Faro, director de Ingeniería de Américas de Forcepoint, afirma que en la empresa, cuentan con una herramienta de seguridad llamada GenAI, una solución integral de seguridad que ofrece visibilidad, control y protección de datos basada en riesgos en plataformas de IA generativa, incluida la integración con ChatGPT Enterprise Compliance de OpenAI.

"Entendemos que las políticas de seguridad de la IA serán tan esenciales para defender la competitividad de una empresa como lo son hoy las políticas de confidencialidad. El objetivo está en conocer exactamente qué aplicaciones utilizan los empleados y con qué datos interactúan, para evitar que estas herramientas dañen los derechos de propiedad de sus contenidos", comentó.

Si bien es cierto que los beneficios que proporciona la inteligencia artificial se vuelven innegables al obtener mayor eficiencia y productividad para las tareas cotidianas, por otro lado, también es necesario analizar lo que representa tener una herramienta o instrumento como este, pues hoy en día aprender más sobre las herramientas de IA generativa se está convirtiendo en una necesidad para mercados como el mexicano, especialmente cuando se trata de seguridad corporativa y los riesgos que conlleva.

## Prevención

La solución de seguridad de GenAI de Forcepoint puede analizar las consultas de los usuarios dentro de las plataformas de IA para identificar y mitigar posibles infracciones, asignando puntuaciones de riesgo basadas en la sensibilidad de la información y garantizando el cumplimiento de los requisitos reglamentarios.

"En resumen, existen varias formas para que los actores maliciosos ejerzan control sobre el entrenamiento de un modelo, desde insertar datos envenenados hasta modificar muestras de entrenamiento existentes. A medida que las organizaciones utilizan la inteligencia artificial y el aprendizaje automático en una gama más amplia de casos de uso, comprender y prevenir dichas vulnerabilidades es de suma importancia", agregó Faro.

Finalmente, Chalala comentó que se tendrá como objetivo dar continuidad a la estrategia de crecimiento de Forcepoint en la región apuntalado a México y Brasil, fomentando entornos seguros y confiables a través de soluciones de seguridad integral que comprendan las identidades digitales y sus comportamientos cibernéticos, a fin de proteger los activos más valiosos de las compañías, sus empleados y los datos críticos, en donde sea que se encuentren.

De cara al 2025, dada la popularidad y adopción de nuevas herramientas de inteligencia artificial y aprendizaje automático, las empresas deben de adoptar soluciones e infraestructura que les permitan operar de manera confiable y sin riesgos, "pues parte de nuestra misión en Forcepoint es poder ofrecer seguridad de datos en todas partes, ayudando a las organizaciones a monitorear y controlar las interacciones de datos dentro de plataformas como ChatGPT Enterprise y otros asistentes de IA", señaló Faro.

Fotos: AdobeStock y Linkedin