Publicado en América Latina el 24/01/2024

# [DigiCert analiza el impacto de la Inteligencia Artificial en la seguridad digital](http://www.notasdeprensa.es)

## Según DigiCert, las herramientas de inteligencia artificial (IA) están ganando cada vez más espacio en la vida y el trabajo

 Con un tamaño de mercado estimado de 102 mil millones de dólares para 2032, no es ningún secreto que la inteligencia artificial (IA) está arrasando en todas las industrias. Sin embargo, la IA requiere datos, y de dónde provienen esos datos, cómo se procesan y qué resulta de esos procesos, requerirá un sentido de identidad y seguridad. Es comprensible que muchas personas estén preocupadas por la seguridad de esos datos. Una encuesta de 2023 encontró que el 81% de los encuestados están preocupados por los riesgos de seguridad asociados con ChatGPT y la IA generativa, mientras que solo el 7% se mostró optimista de que las herramientas de IA mejorarían la seguridad en Internet. Por lo tanto, las medidas estrictas de ciberseguridad serán aún más críticas con las tecnologías de inteligencia artificial. "Existen innumerables oportunidades para aplicar la IA en la ciberseguridad para mejorar la detección de amenazas, la prevención y la respuesta a incidentes. Por lo tanto, las empresas deben comprender las oportunidades y debilidades de la IA en ciberseguridad para adelantarse a las próximas amenazas", afirmó Avesta Hojjati - Vicepresidente de Ingeniería y Jefe de I+D de DigiCert. Usando la IA El lado positivo es que la IA puede ayudar a transformar la ciberseguridad con respuestas más efectivas, precisas y rápidas. Algunas de las formas en que se puede aplicar la IA a la ciberseguridad incluyen: Reconocimiento de patrones para reducir falsos positivos: la IA es excelente en el reconocimiento de patrones, lo que significa que puede detectar mejor anomalías y proporcionar un análisis de comportamiento y detectar amenazas en tiempo real. De hecho, un estudio del Ponemon Institute realizado en 2022 encontró que las organizaciones que utilizan sistemas de detección de intrusiones impulsados ​​por IA experimentaron una reducción del 43 % en los falsos positivos, lo que permitió a los equipos de seguridad centrarse en amenazas genuinas. Además, se demostró que las soluciones de seguridad del correo electrónico basadas en IA reducen los falsos positivos hasta en un 70%. Permitir la escala mejorando las capacidades humanas: la IA se puede utilizar para mejorar las capacidades humanas, proporcionar un tiempo de respuesta más ágil y ofrecer escalabilidad. La única limitación a la escala será la disponibilidad de datos. Además, los chatbots de IA se pueden utilizar como asistentes virtuales para ofrecer soporte de seguridad y aliviar parte de la carga de los agentes humanos. Acelerar la respuesta y recuperación ante incidentes: la IA puede automatizar acciones y tareas rutinarias basadas en capacitación previa y recopilación de datos multipunto, ofrecer tiempos de respuesta más rápidos y reducir las brechas de detección. La IA también puede automatizar los informes, ofreciendo información a través de consultas en lenguaje natural, simplificando los sistemas de seguridad y brindando recomendaciones para mejorar futuras estrategias de ciberseguridad. Capacitación sobre phishing en sandbox: la IA generativa puede crear escenarios de phishing realistas para capacitación práctica en ciberseguridad, fomentando una cultura de vigilancia entre los empleados y preparándolos para las amenazas del mundo real. Alerta rojaAhora se ve que los atacantes utilizan la IA en sus ataques. Por ejemplo: Campañas de malware automatizadas con IA: los ciberdelincuentes pueden emplear IA generativa para crear malware sofisticado que ajuste el comportamiento para evitar la detección. Estas cepas de malware "inteligentes" son más difíciles de predecir y controlar, lo que aumenta el riesgo de interrupciones generalizadas del sistema y violaciones masivas de datos. Ataques de phishing avanzados: la IA generativa tiene la capacidad de aprender e imitar el estilo de escritura y la información personal de un usuario, lo que hace que los ataques de phishing sean considerablemente más persuasivos. Los correos electrónicos de phishing personalizados, que parecen provenir de contactos confiables o instituciones acreditadas, pueden engañar a las personas para que divulguen información confidencial, lo que representa una amenaza sustancial para la ciberseguridad personal y corporativa. Deepfakes realistas: gracias a la IA generativa, los actores malintencionados ahora pueden crear deepfakes: falsificaciones de imágenes, audio y vídeos muy convincentes. Los deepfakes plantean un riesgo importante de campañas de desinformación, actividades fraudulentas y suplantación de identidad. Imagine un vídeo notablemente realista de un director ejecutivo anunciando una quiebra o una grabación de audio fabricada de un líder mundial declarando la guerra. Estos escenarios ya no se limitan al ámbito de la ciencia ficción y tienen el potencial de causar perturbaciones significativas. Además, la IA requiere una gran cantidad de datos y las empresas deben limitar exactamente lo que se comparte, ya que crea otro tercero donde los datos podrían verse afectados. Incluso el propio ChatGPT sufrió una violación de datos debido a una vulnerabilidad en la biblioteca de Redis, que permite a los usuarios acceder al historial de chat de otros. OpenAI resolvió rápidamente el problema, pero resalta los riesgos potenciales para los chatbots y los usuarios. Algunas empresas han comenzado a prohibir por completo el uso de ChatGPT para proteger datos confidenciales, mientras que otras están implementando políticas de IA para limitar los datos que se pueden compartir con la IA. ¿Cómo generar confianza digital en la IA con PKI?El uso de tecnologías como la infraestructura de clave pública (PKI) puede desempeñar un papel fundamental en la protección contra amenazas emergentes relacionadas con la IA, como las falsificaciones profundas, y en el mantenimiento de la integridad de las comunicaciones digitales. Por ejemplo, un consorcio de actores líderes de la industria, incluidos Adobe, Microsoft y DigiCert, están trabajando en un estándar conocido como Coalición para la procedencia y autenticidad del contenido (C2PA). Esta iniciativa introdujo un estándar abierto diseñado para abordar el desafío de verificar y confirmar la legitimidad de los archivos digitales. C2PA aprovecha PKI para generar un rastro indiscutible, lo que permite a los usuarios discernir entre medios genuinos y falsificados. Esta especificación brinda a los usuarios la capacidad de determinar la fuente, el creador, la fecha de creación, la ubicación y cualquier modificación de un archivo digital. El objetivo principal de este estándar es fomentar la transparencia y la confiabilidad en los archivos multimedia digitales, especialmente dada la creciente dificultad para distinguir el contenido generado por IA de la realidad en el entorno actual. "En resumen, la IA desarrollará muchas oportunidades en ciberseguridad y apenas se ha rozado la superficie de lo que puede hacer. La IA se utilizará como herramienta tanto ofensiva como defensiva para prevenir y provocar ciberataques. Pero la clave es que las empresas sean conscientes de los riesgos y empiecen a implementar soluciones ahora, teniendo en cuenta que la IA no puede sustituir completamente a los humanos", concluye Hojjati.

**Datos de contacto:**

DigiCert Latam

Digicert Latam

3125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/digicert-analiza-el-impacto-de-la-inteligencia](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica Software Ciberseguridad Innovación Tecnológica Digital



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)