La inteligencia artificial: ¿una amenaza o una oportunidad para la ciberseguridad?

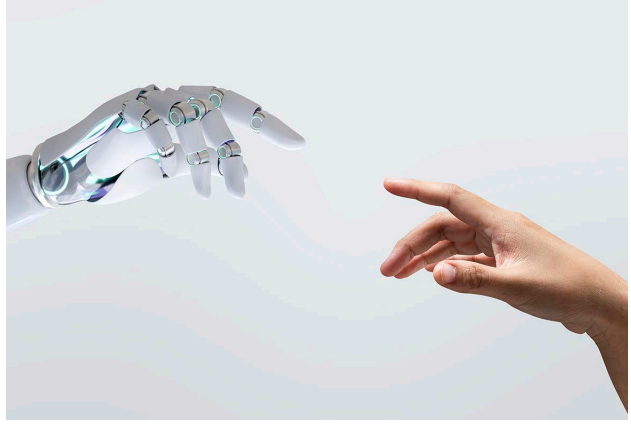
¿Has subido tu fotografía para crear una versión digitalizada con apoyo de la inteligencia artificial? ¿Cuál es el riesgo?

La inteligencia artificial es una tecnología que puede ser muy útil para las empresas y las personas, pero también puede presentar riesgos si no se gestiona adecuadamente. Uno de los riesgos más preocupantes es el potencial de la inteligencia artificial para ser utilizada con fines malintencionados.

Durante este mes, aplicaciones que hacen uso de la inteligencia artificial han tomado los reflectores particularmente con herramientas como convertir una serie de fotografías para mejorar y optimizarlas o hasta crear arte con ellas. Pero también herramientas como ChatGPT que permite interactuar por medio de conversaciones y obtener información en un lenguaje sencillo.

La inteligencia artificial puede ser utilizada para crear sistemas que simulan comportamientos humanos de manera realista. Esto puede ser muy útil para mejorar la atención al cliente o para realizar tareas repetitivas en una empresa. Sin embargo, también puede ser utilizada con fines malintencionados, como la creación de falsas identidades o la difusión de noticias falsas, incluyendo los deepfakes (videos).

El riesgo de subir fotografías para hacer uso de herramientas que crean arte con inteligencia artificial es que **la fotografía puede ser utilizada sin el permiso del dueño.** Quizá el mayor riesgo es que almacenen información sobre la persona, es decir, sus biométricos. Pero también puede ser que la empresa que tiene el algoritmo, no lo haga: no los sabremos.



Si bien existen muchos riesgos desde el punto de vista personal al estar compartiendo fotografías o información de que la misma inteligencia digital va a ir aprendiendo, pocas veces se habla de los riesgos para la organización.

La inteligencia artificial puede ser utilizada para realizar ataques cibernéticos más sofisticados y difíciles de detectar. Por ejemplo, un sistema de inteligencia artificial podría utilizarse para realizar ataques de phishing o para infiltrarse en sistemas de seguridad. El nivel de realismo que puede incorporar preocupa entre los especialistas.

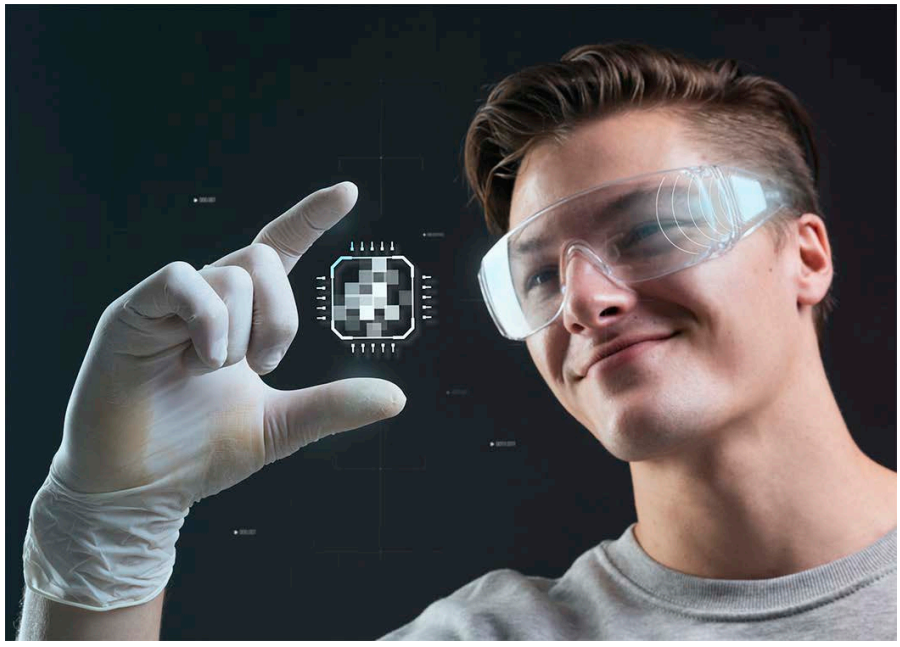
Los ciberatacantes o aquellos que no son tan versados, podrían utilizar la inteligencia artificial para aprender y adaptarse a las medidas de ciberseguridad utilizadas por una empresa, lo que podría permitirles acceder a información confidencial o realizar acciones malintencionadas sin ser detectados. Hoy es posible pedirle a alguna de estas plataformas de inteligencia artificial, el código para poder afectar un sistema; no en todos los casos funciona, pero por lo menos lo intenta.

Aunque la inteligencia artificial puede ser una herramienta muy útil para las empresas, es importante tomar medidas de seguridad adecuadas para proteger la información confidencial y evitar posibles ataques cibernéticos. La alta administración debe considerar estos riesgos y tomar las medidas necesarias para gestionarlos adecuadamente.

Para poder protegerse no hay más que seguir con lo que se tiene actualmente: **realizar un análisis de riesgos para identificar vulnerabilidades y debilidades** en la ciberseguridad de la organización, implementar medidas de ciberseguridad adecuadas y capacitar colaboradores en temas de ciberseguridad.

Si está pensando en incorporar inteligencia artificial en su organización, el análisis de riesgo de cómo alguien podría aprovechar esa tecnología para obtener un beneficio será necesario.

Pero también podría hacer uso de la inteligencia para poder realizar análisis de riesgos de ciberseguridad, detección de amenazas como phishing o la identificación de malware que pueda infiltrarse en la organización; pero quizá lo que más se usa hoy en día la inteligencia artificial en ciberseguridad es para **poder prevenir ataques:** una vez detectadas las amenazas, la inteligencia digital puede ayudar a prevenir que estos ataques tengan éxito. Esto puede incluir la integración de herramientas de control con la monitorización en tiempo real.



Como todo, hay cosas buenas y malas. Depende de nosotros identificar el riesgo. Lo más irónico: esta columna se realizó haciendo uso de inteligencia artificial, si bien tuve que modificar algunas cosas y redactarlas de una forma diferente, la esencia fue a partir de la pregunta: **¿cuáles son los riesgos de la inteligencia artificial para las empresas desde el punto de vista de ciberseguridad?**

Adicional: si usted ya subió sus 20 fotografías para crear las imágenes apoyado con la inteligencia artificial, no se preocupe, no vale la pena. Si estaba esperando a hacerlo, **identifique los riesgos y decida,** pero si lo hace, hágalo en una plataforma confiable y lea detenidamente los términos y condiciones de uso para conocer lo que harán con las fotografías.

Autor: Andrés Velazquez
Fuente de información: www.forbes.com