

8 desafíos de la adopción de Inteligencia Artificial en las empresas



Rhett Nieto, gerente de Tecnología y Ciberseguridad de FEMSA ARMUR, se unió como ponente en la semana de ciberseguridad 2024

11/11/2024

LiveTEC

Shutterstock

¿Cuáles son los retos y amenazas actuales de la inteligencia artificial (IA)?

Omar Tolentino, director de Ciberseguridad en el [Tec de Monterrey](#), explicó que la inteligencia artificial (IA) es una **herramienta irremplazable en el contexto actual**, pero indicó que esta **no está exenta de fallas**.

A pesar de que la IA todavía no ha alcanzado un nivel de autonomía total, el EXATEC **Rhett Nieto**, gerente de Tecnología y Ciberseguridad de **FEMSA ARMUR**, advierte que esta continúa **evolucionando de manera vertiginosa semana tras semana**.

Como parte de la [Cybersecurity Week 2024](#), el EXATEC compartió con la audiencia como esta **tecnología es un elemento clave para la transformación del futuro** que a su vez debe ser utilizado con su debido **cuidado y ética**.



Rhett Nieto fue uno de los panelistas durante la Semana de Ciberseguridad. Foto: Live Tec

*“El **mejor activo que tenemos es el conocimiento**. El conocimiento es nuestra primera y última línea de defensa ante el tipo de amenazas que puede traer la IA”, expresó Tolentino como preámbulo a la charla de Nieto.*

*“Existen muchos **beneficios alrededor de la adopción de la IA**, como la innovación y la ventaja competitiva y las tomas de decisiones basadas en datos, pero **eso también implica vulnerabilidades**”, aclaró Nieto.*

Desafíos en la adopción de la IA en empresas

Nieto compartió los retos que enfrentan las empresas al adoptar la IA:

1. Integración con sistemas existentes

*“Se refiere a la manera en la que se **incorporan soluciones de IA como parte de las infraestructuras tecnológicas** y los sistemas de información que ya existen”,* explicó Nieto.

En dicho caso, el experto expresa como este proceso, a pesar de que es fundamental, va a **requerir una alocación de tiempo y recursos adicionales**.

2. Escasez de talento personalizado

De acuerdo con el experto, la **demanda actual de profesionistas con formación en el uso de IA supera todavía a la oferta** en el mercado laboral.

*“Esto dificulta el **encontrar y retener talento** para desarrollar e implementar soluciones de IA”,* explicó.

3. Amenaza ante la privacidad y seguridad de datos

A medida que las empresas **dependen más de datos** para el desarrollo de sus estrategias de IA, **más vulnerables son a ataques cibernéticos** y robo de información.

*“Las corporaciones tienen que **asegurarse de que sus aplicaciones de IA respeten la privacidad de datos** y eviten sesgos algorítmicos que puedan ser injustos o discriminatorios”,* enfatizó Nieto.

4. Resistencia organizacional ante el cambio

*“La inserción de la IA puede **generar temores entre los empleados**”,* reflexionó Nieto.

Según Nieto, este miedo, usualmente proveniente de generaciones más avanzadas en edad, se da por la **percibida amenaza del reemplazo de sus roles por la IA**.

5. Regulación y cumplimiento

En este punto, Nieto destaca la **falta de regulación jurídica en cuanto al uso de IA**, particularmente en México donde no hay leyes oficiales al respecto.

De tal forma, el especialista señala que el panorama en este sentido es ambiguo y, por ende, las **sanciones ante el mal uso de IA pueden resultar complejas**.



Riesgos vinculados a modelos de lenguaje de IA generativa

6. “Inyección” de *prompts*

Nieto explica que un ataque proveniente de un modelo de lenguaje puede darse si el **atacante logra manipular los *prompts* alimentados y con ello extraer información** a través de chatbots, filtración de datos, emails, etc.

Un *prompt* es una instrucción o frase inicial que se le da a una inteligencia artificial o sistema generativo para guiar su respuesta o producción de contenido, como texto, imagen o código.

*“El problema es que hay **bases de datos creadas para convencer a los modelos** más comerciales como ChatGPT, Gemini, etc., a que **ejecuten acciones que no están programados** para realizar normalmente”,* explicó Nieto.

7. Entrenamiento para “envenenar” datos

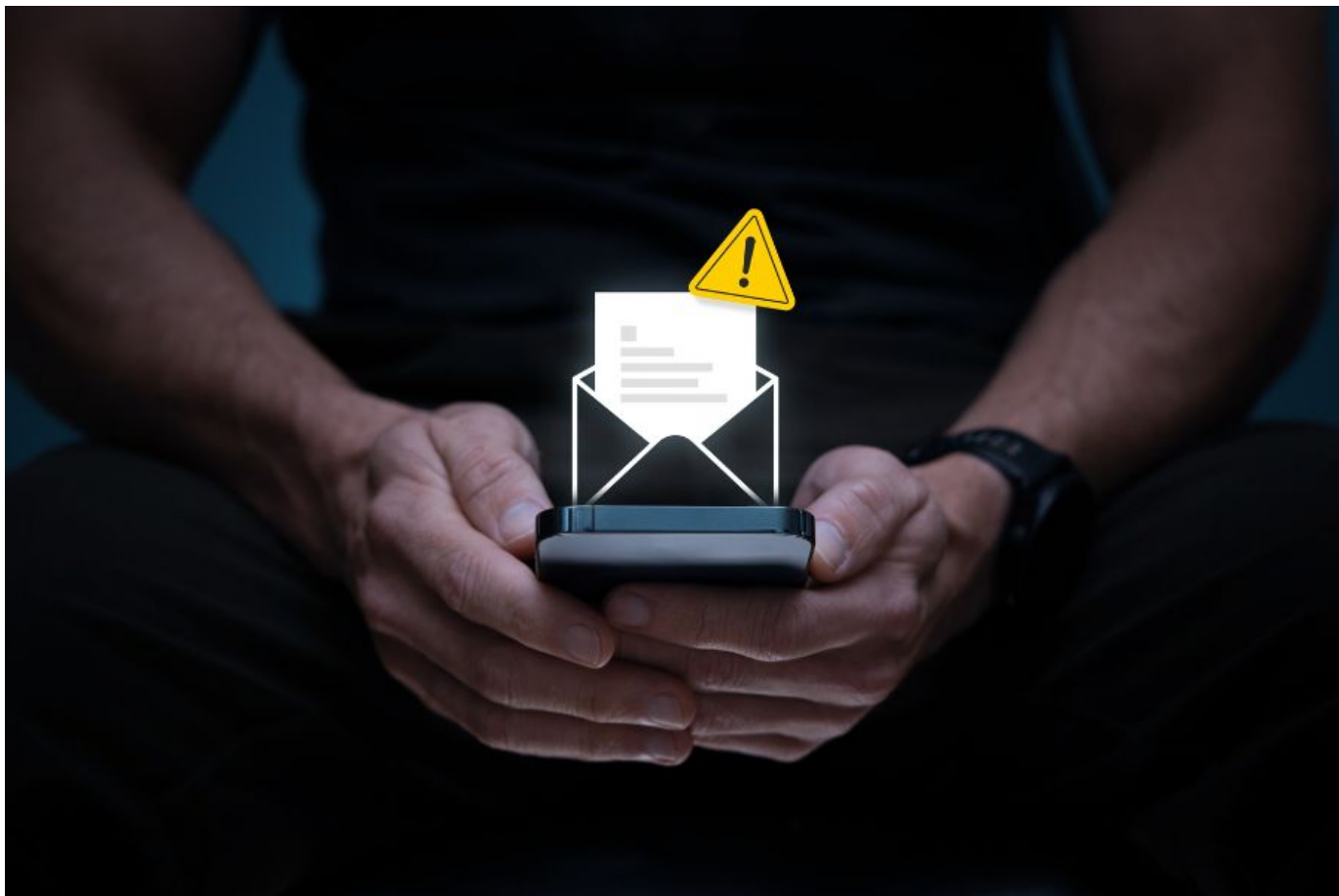
En este caso, el modelo se ve amenazado al **introducir sesgos o puertas traseras que comprometan su seguridad**, efectividad o comportamiento bajo los lineamientos éticos programados.

*“Todo depende de **¿cómo entrenaste al modelo y con qué datos le enseñaste a funcionar?** Porque los datos pueden ser manipulados desde el inicio e incluso crear atajos secretos para ciertas personas”,* aclaró.

8. Falta de transparencia

Esto puede impactar el proceso de toma de decisiones de un modelo, remarcó el experto, indicando que **si no se conocen los lineamientos que este sigue para actuar, es posible que estos puedan caer en faltas éticas**.

*“El ejemplo más claro está en los **sistemas de seguridad que utilizan reconocimiento facial** donde se han dado casos de discriminación racial automatizada que provenía desde el mismo sistema”,* compartió.



9. Creación de *deepfakes*

Desde la cara de una celebridad hasta la voz de tu empleador, el experto indica que los **deepfakes son una de las amenazas más visibles de la IA generativa** actualmente y su potencial para evolucionar puede ser preocupante.

*“Con herramientas que incluso ya son gratuitas, una **persona maliciosa puede crear una foto o video de una persona que nunca grabó** o imitar la voz de alguien con tan solo unas muestras de audio”, advirtió el experto.*

10. Negación de servicio

En este escenario, expresó Nieto, los atacantes pueden **interferir con el modelo** de manera en la que **consume una cantidad excesiva de recursos**.

*“Además de que va a impactar la calidad de servicio del modelo (al saturarse), el resultado más común es la **generación de altos costos de funcionamiento**”, dijo el ponente.*

Finalmente, ante un panorama de amenazas aparentemente infinito, el panelista **alienta a las personas a no temerle a la IA**, ya que simplemente es cuestión de:

- *Educarse sobre las capacidades y limitaciones de la misma*
- *Evitar introducir datos sensibles (propios o de empleados)*
- *Mantener un monitoreo firme en las soluciones o modelos que se utilicen*
- *Limitando el acceso a usuarios autorizados*
- *Establecer principios y lineamientos éticos firmes*
- *Actualizar las herramientas para mantener sus sistemas de seguridad vigentes*

Cybersecurity Week 2024

Durante una semana del **4 al 8 de noviembre, expertos en ciberseguridad**, tanto nacionales como internacionales compartieron sus conocimientos sobre amenazas, detección y tips para proteger datos y la integridad digital.

Los temas que se abordaron a través de 10 conferencias fueron: inteligencia artificial, navegación segura, tendencias de ciberseguridad en México, ransomware, estafas digitales, entre otras.

Puedes ver la retransmisión por **LIVE.TEC**: <https://live.tec.mx/cbweek>.

TAMBIÉN TE PUEDE INTERESAR:

