

Inteligencia Artificial en la Ciberseguridad



La ciberseguridad tiene un gran impacto en la seguridad nacional, por lo que los gobiernos están invirtiendo en nuevas tecnologías para reducir el riesgo de acceso no autorizado y prevenir ciberataques a sus activos digitales.



De acuerdo al informe Wilson Center, México es el segundo país en América Latina con el mayor número de ciberataques en los últimos años.

En 2023 se reportaron aproximadamente 80,000 ciberataques individuales y empresariales en el país.

Algunos Tipos de Ciberataques



Malware

Programa malicioso diseñado para dañar intencionalmente un sistema computacional o recabar datos de interés sin el conocimiento del usuario.



Ransomware

Programa que bloquea o restringe el acceso a los archivos del sistema operativo y pide un pago a cambio de eliminar esta restricción.

Phishing

Método para obtener información sensible o confidencial de los usuarios haciéndose pasar por una entidad confiable a través de un correo o llamada telefónica.



Explotación Día cero

Técnica de ataque contra una aplicación o sistema computacional a partir de obtener conocimiento de vulnerabilidades desconocidas incluso por los usuarios o fabricantes.



Inyección SQL

Método de infiltración de código donde el atacante usa un segmento de código SQL para manipular la base de datos y acceder a información potencialmente valiosa.



Ataque XSS (Cross Site Scripting)

Permite que el atacante ejecute código malicioso en el navegador de otro usuario.

¿Cómo contribuye la IA ?

1

Identificando patrones de comportamiento sospechosos y maliciosos que ayuden a la prevención, detección y resolución de problemas de seguridad en tiempo real.



2

Haciendo predicciones sobre los futuros movimientos de los atacantes basado en experiencias anteriores.

Haciendo uso del Aprendizaje Máquina como una tecnología clave para desarrollar sistemas inteligentes en el contexto de la ciberseguridad.

3

¿Cuál es el futuro de la ciberseguridad con la IA?



La IA podría usar datos históricos para predecir con mayor precisión los tipos de ataques cibernéticos y prepararse para ellos.



La IA podría automatizar la gestión de amenazas y permitir que los especialistas en ciberseguridad desarrollen estrategias más efectivas y de alto nivel.



La IA podría usarse para garantizar la privacidad de la información de los usuarios al detectar y bloquear el seguimiento no autorizado y la recopilación de datos personales.



La IA podría ser usada junto con otras tecnologías como Blockchain para almacenar y transferir información de forma segura en un ambiente descentralizado.