LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD: PREVENCIÓN Y DETECCIÓN DE AMENAZAS EN LA ERA DIGITAL

Luis Alberto Flores Montaño, Dr.[1], Jacobo Sandoval Gutiérrez, Dr.[1]
[1]Universidad Autónoma Metropolitana, Unidad Lerma
lfloresm1703o@alumno.ipn.mx, j.sandoval@correo.ler.uam.mx

Boletín No. 107, 1o. de marzo de 2025

Resumen

Hoy en día la ciberseguridad es una preocupación creciente en un mundo altamente conectado, donde las ciberamenazas evolucionan constantemente en su complejidad y sofisticación, afectando a diversos sistemas tanto complejos o de bajo procesamiento, afectando a la población en general y a diversas organizaciones. En este artículo se explora como la inteligencia artificial (IA) puede ser funcional en la rama de la ciberseguridad, destacando el potencial y la capacidad para detectar, prevenir y recuperarse de los ataques cibernéticos en tiempo real. Además, se analizan casos prácticos de herramientas que actualmente son utilizadas para la protección de datos utilizando la inteligencias artificial; adicionalmente, se detallan ventajas y desafíos de integrar la IA en sistemas que protejan la seguridad de los dispositivos, adicionalmente, se explora el potencial que se tiene para transformar el panorama de la ciberseguridad si bien la IA ofrece soluciones que pueden ser prometedoras, también plantea algunos retos tanto éticos como técnicos, los cuales deben abordarse para garantizar su eficacia y eficiencia.

Palabras Clave: inteligencia artificial, ciberseguridad, prevención de amenazas, detección de malware, seguridad digital.

1. Introducción

En la época digital actual, los ciberataques se han vuelto más frecuentes y sofisticados, afectando a diversas organizaciones. Desde ataques sencillos como de ataques de fuerza bruta o de ransomware hasta violaciones de datos a gran escala como lo son ataques DDoS o ataques de día cero (Anderson, 2023); todas y cada una de estas ciberamenazas ponen en peligro la integridad, confidencialidad y disponibilidad, así como la privacidad de cada individuo u organizaciones, riesgos en la economía y en la seguridad global. Teniendo en cuenta esta realidad, la IA ha emergido como una herramienta clave para combatir estos riesgos ante ciberataques (Wirkuttis, 2017). Con capacidades como el aprendizaje automático y la detección de patrones anómalos, la IA está revolucionando la forma en que se identifica y previene ciberataques. En este artículo se analizan las aplicaciones que tiene la IA en la ciberseguridad, resaltando la importancia de la detección en tiempo real y la respuesta proactiva a amenazas.

En la figura 1, se muestra algunos de los beneficios y aportes que tiene la IA dentro de la ciberseguridad, este tecnología puede llevar diversos avances como lo es la detección y prevención de fugas de correos como lo es el phishing y el spamming, se pueden prevenir ataques sofisticados como los de día cero, se puede realizar una autenticación más precisa sobre la autorización de los usuarios a ciertas aplicaciones o programas específicos, así mismo se puede hacer la detección de diversos malwares y de vulnerabilidades dentro de un sistema, esto con el fin de tener una seguridad preventiva para las amenazas existentes; adicionalmente, se puede tener un análisis de eventos que se registra en la actividad de los usuarios, y alertar al sistema de monitoreo.

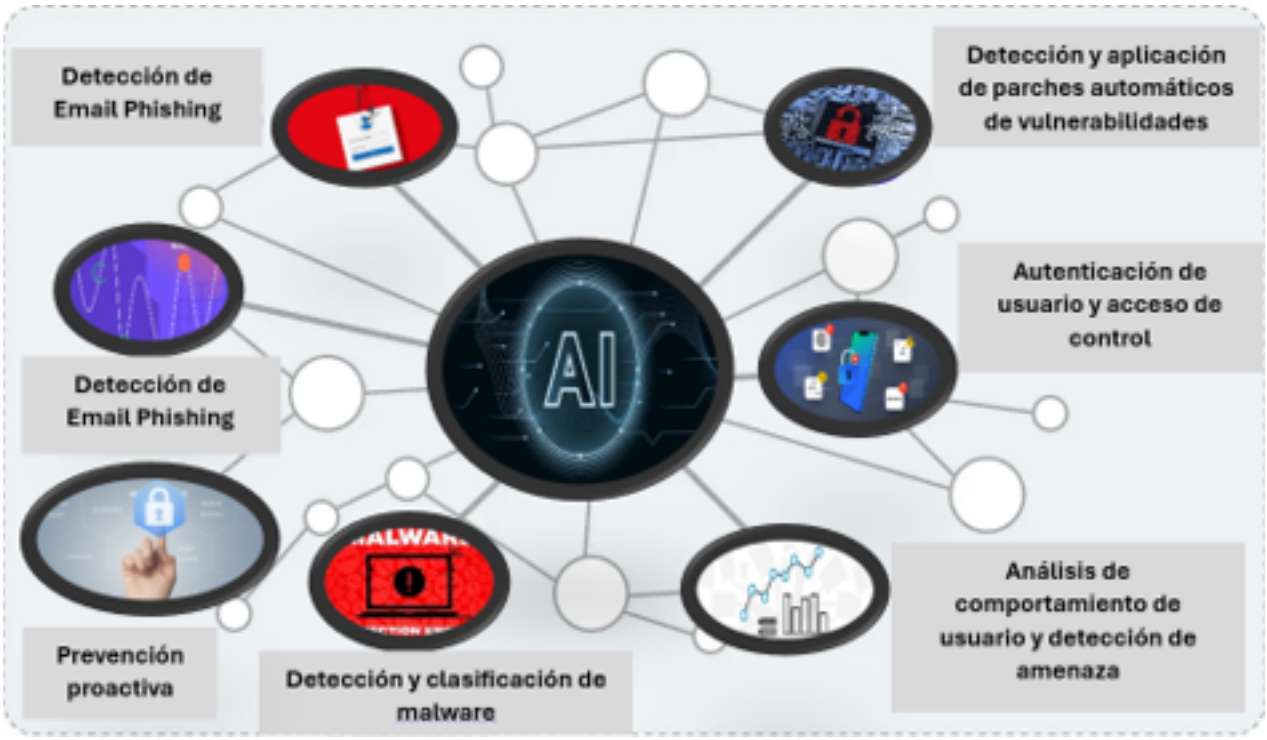

Figura 1 Funciones de la IA dentro de la ciberseguridad (Elaboración propia).

2. Contenido del artículo

A continuación, se describe de manera precisa las funciones de la IA dentro de la ciberseguridad, mostradas en la figura 1.

1. **El papel de la IA en la detección de amenazas:** La IA permite analizar grandes volúmenes de datos en tiempo real, identificando patrones anómalos que podrían indicar actividades maliciosas. Herramientas basadas en IA, como son los sistemas de detección y prevención de intrusiones (por sus siglas en inglés IDS/IPS), emplean algoritmos de aprendizaje automático para diferenciar el tráfico normal del malicioso (Zhang, 2023). Un ejemplo de esto es el uso de redes neuronales profundas para detectar intentos de envío de correos con contenido phishing, esto es prevenido antes de que lleguen al usuario final.
2. **Detección de Email Phishing:** Se puede identificar los correos fraudulentos diseñados para engañar a los usuarios y robar las credenciales o información sensible; con técnicas de inteligencia artificial se puede realizar diversas detecciones para este tipo de correos como lo es el procesamiento de lenguaje natural (NLP), para el análisis de contenido detectando patrones maliciosos, esto puede involucrar errores gramaticales, solicitudes de información o enlaces maliciosos (Cylance, 2023).
3. **Prevención proactiva mediante IA:** Además de detectar amenazas y correos maliciosos, la IA también puede anticiparse a ataques futuros al analizar tendencias históricas y comportamientos sospechosos. Por ejemplo, sistemas de IA pueden identificar vulnerabilidades potenciales en la infraestructura digital y sugerir soluciones antes de que sean explotadas (Darktrace, 2023).
4. **Detección y aplicación de parches automáticos de vulnerabilidades IA:** También la IA puede identificar vulnerabilidades en sistemas y automatiza las descargas e instalación de parches sin intervención humana. Un ejemplo de esto es emplear algoritmos para predecir las vulnerabilidades futuras o priorizar parches acordes con el impacto que se pudiera generar ante ciertas amenazas, con esto reduce la exposición ante ataques del día cero (Darktrace, 2023).
5. **Autenticación de usuario y control de acceso IA:** Además de diversas detecciones y prevenciones que se pueden realizar con ayuda de esta tecnología, también es posible la autenticación para garantizar que

solo los usuarios autorizados accedan a recursos específicos según los permisos. Por ejemplo, la IA puede realizar autenticaciones basadas en el comportamiento, donde algoritmos de redes neuronales pueden detectar patrones como la velocidad de tecleo, movimientos del ratón o interacción con dispositivos para detectar ciertas anomalías (Cylance, 2023).

6. **Análisis de comportamiento de usuario y detección de amenazas IA:** Teniendo en cuenta la detección de patrones, también es posible hacer un análisis y monitoreo completo del comportamiento del usuario para poder detectar actividades anómalas que podrían indicar amenazas internas o externas, un ejemplo de esto es el uso de algoritmos de aprendizaje no supervisado para detectar patrones fuera de lo común (Cylance, 2023).

3. Casos prácticos de IA en ciberseguridad

De lo mencionado anteriormente, se retoman casos prácticos de herramientas que utilizan este tipo de tecnologías dentro de la industria. A continuación, se mencionan algunas de estas.

- **Detección de malware:** Herramientas dentro de la industria como es Cylance utiliza la IA para analizar código de archivos y predecir si son maliciosos, incluso sin firmas conocidas (Cylance, 2023).
- **Respuestas automatizadas:** Sistemas como lo es Darktrace también utilizan la IA para contener ataques en tiempo real, con el propósito de aislar dispositivos comprometidos sin intervención humana (Darktrace, 2023).
- **Protección contra ataques de fuerza bruta:** Como se mencionó anteriormente, la IA puede identificar patrones de intentos de acceso repetidos y bloquearlos automáticamente, dentro de la industria existen diversas herramientas encargadas de detectar ataques de este tipo encargados de la detección temprana, adaptabilidad, reducción de falsos positivos y acciones tempranas, algunas de estas son Fail2Ban con IA, Elastic Security o Azure Sentinel (Pooyandeh, 2022).

4. Desafíos y limitaciones

A pesar de observar diversas ventajas, la otra cara de la moneda es que la IA también enfrenta retos en el ámbito de la ciberseguridad. Algo que es de suma importancia es la calidad de los datos de entrenamiento, ya que al tener datos incompletos o sesgados pueden generar falsas alarmas, y, por lo tanto, pasar por alto amenazas reales. Por otro lado, los ciberdelincuentes también utilizan IA para desarrollar ataques más sofisticados, lo que genera una carrera armamentista tecnológica. Finalmente, surgen dilemas éticos sobre el uso de IA en la vigilancia y el monitoreo, que podrían invadir la privacidad de los usuarios (Ansari, 2022).

5. Conclusiones

La integración de la inteligencia artificial en la ciberseguridad representa un avance fundamental para la prevención y detección de amenazas en la era digital. Su capacidad para analizar grandes volúmenes de información y reconocer patrones en tiempo real permite neutralizar ataques sofisticados de manera más proactiva. No obstante, para maximizar estos beneficios resulta imperativo hacer frente a sus limitaciones técnicas, como el sesgo en los datos de entrenamiento, así como a los desafíos éticos relacionados con la privacidad y la vigilancia, garantizando con ello un entorno digital no sólo más seguro, sino también responsable y confiable.

Referencias

[1] Anderson, B. et al. (**2023**). *.AI-Driven Cybersecurity: Trends and Challenges."* Journal of Information Security.

[2] Ansari, M. F. et. al. (**2022**). *The impact and limitations of artificial intelligence in cybersecurity: a literature review.* International Journal of Advanced Research in Computer and Communication Engineering.

[3] Cylance. (**2023**). *"How AI is Changing Malware Detection."* Disponible en: `www.cylance.com`.

[4] Darktrace. (**2023**). *.Autonomous Response to Cyber Threats Using AI."* Disponible en: `www.darktrace.com`.

[5] Pooyandeh, M. et. al. (**2022**). *Cybersecurity in the AI-Based metaverse: A survey* Applied Sciences. 12(24), 12993.

[6] Wirkuttis, N., & Klein, H. (**2017**). *Artificial intelligence in cybersecurity.* Cyber, Intelligence, and Security.

[7] Zhang, Y. et al. (**2023**). *"Machine Learning for Network Intrusion Detection."* IEEE Transactions on Cybernetics.

Flores Montaño, L. A., Sandoval Gutiérrez, J. *(2026). LA INTELIGENCIA ARTIFICIAL EN LA CIBERSEGURIDAD: PREVENCIÓN Y DETECCIÓN DE AMENAZAS EN LA ERA DIGITAL. Boletín UPIITA. año XX, (NÚM) 2026.*