Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **Doce**

Febrero: Riesgos de IA en el contexto de la Ciberseguridad

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CIP – CSIRT Académico UNAD

E-boletín Informativo CIP- CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Doce
Febrero de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Hernando José Peña Hidalgo
Docente Esp. Seguridad Informática UNAD

Estado legal:
Periodicidad: Quincenal
ISSN: 2806-0164

Licencia Atribución – Compartir igual

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 12 4
Introducción 4
Desarrollo 5
¿Qué es la inteligencia artificial?: 5
¿Cuáles son los vectores de ataque más usados por los ciberdelincuentes? 5
¿Cómo hacer uso de la IA en un contexto organizacional para reducir la exposición al riesgo? 6
Tips para hacer buen uso de la IA en la vida personal y en un espacio organizacional 7
Canales de comunicación 8
Bibliografía Propuesta 9

Boletín informativo Número 12

Febrero 25 de 2023

Riesgos de IA en el contexto de la Ciberseguridad

Autores:

Fernando Zambrano Hernández
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

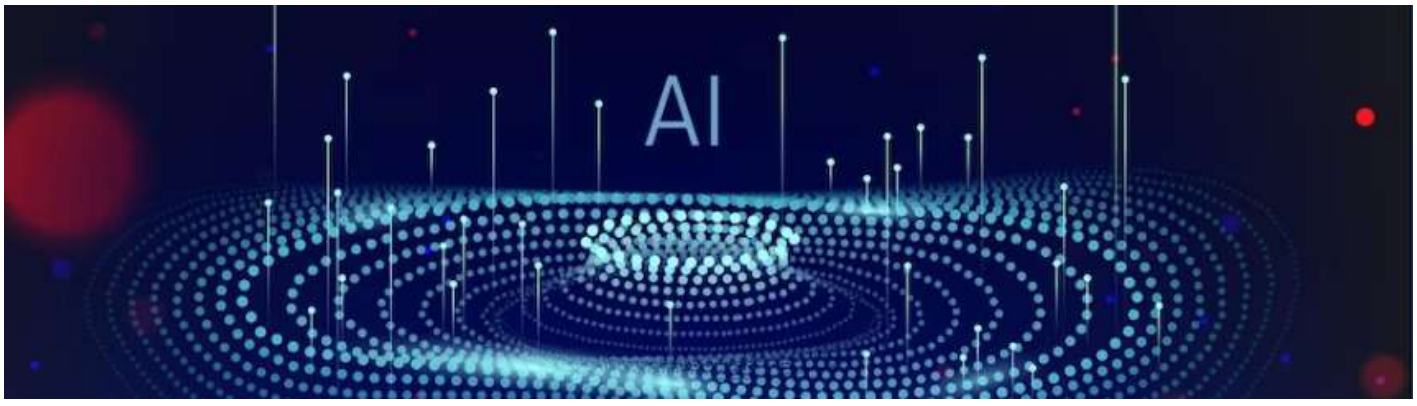
John Fredy Quintero Tamayo
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0003-0128-1214

Néstor Raúl Cárdenas Corral
CIP – CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

En los últimos años, la inteligencia artificial (IA) ha tenido un gran impacto en la ciberseguridad, tanto en la detección de amenazas como en la respuesta a ellas. Según un estudio realizado por la firma de seguridad McAfee en 2020, el uso de IA y aprendizaje automático ha aumentado en un 71% en el sector de la seguridad cibernética en comparación con el año anterior. Además, la IA se está utilizando cada vez más para prevenir ataques, mejorar la eficacia de los sistemas de seguridad y mitigar los riesgos[1].

Por otro lado, la IA también está siendo utilizada por los ciberdelincuentes para llevar a cabo ataques más sofisticados y personalizados, lo que ha llevado a la necesidad de desarrollar sistemas de defensa más avanzados. Según un informe de la consultora Accenture de 2021, el 66% de los profesionales de seguridad cibernética[2]. encuestados afirmaron que los ciberdelincuentes están utilizando cada vez más la IA para llevar a cabo ataques.

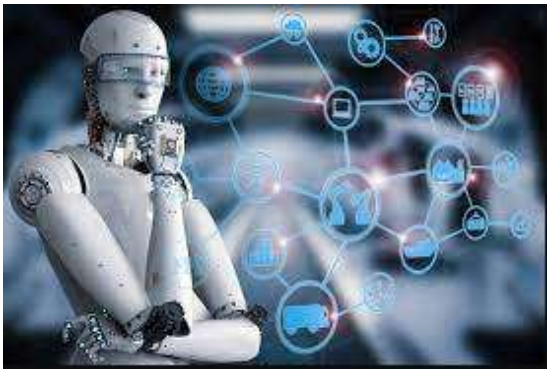


[1] McAfee. (2020). McAfee uncovers major increase in use of external attacks and collaboration by cyber criminals. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-threats-evolving-mcafee.pdf

[2] Accenture. (2021). State of cyber resilience 2021: Enhancing cyber resilience through AI and automation. https://www.accenture.com/_acnmedia/pdf-149/accenture-state-of-cyber-resilience-2021.pdf#zoom=50

Desarrollo

¿Qué es la inteligencia artificial?:



Recuperado de: https://martinbrainon.com/inicio/la-inteligencia-artificial-es-el-futuro-de-la-ciberseguridad/

La Inteligencia Artificial (IA) es un área de la informática que se enfoca en desarrollar algoritmos y técnicas computacionales capaces de imitar la inteligencia humana y realizar tareas que antes solo podían ser realizadas por humanos. En la actualidad, la IA está presente en diversos ámbitos, como la medicina, la educación, la industria y, por supuesto, la ciberseguridad.

En el campo de la ciberseguridad, la IA está siendo utilizada para prevenir y mitigar las amenazas cibernéticas. Por ejemplo, los sistemas de detección de intrusiones (IDS) basados en IA pueden analizar grandes volúmenes de datos en tiempo real para identificar patrones y anomalías que puedan indicar un ataque. También se están utilizando sistemas de aprendizaje automático para analizar el tráfico de red y detectar comportamientos sospechosos, como el tráfico malicioso o la actividad de los botnets.

Además, la IA también se está utilizando para mejorar la eficacia de los sistemas de seguridad de ciberseguridad. Por ejemplo, se están desarrollando algoritmos de aprendizaje automático para identificar vulnerabilidades en el software y en las infraestructuras de red, lo que permite a los expertos en seguridad actuar antes de que un atacante aproveche estas vulnerabilidades.

Por otro lado, la IA también se está utilizando por los ciberdelincuentes para llevar a cabo ataques más sofisticados y personalizados. Por lo tanto, es importante que los expertos en ciberseguridad estén al tanto de las amenazas potenciales que la IA puede presentar y desarrollen medidas de seguridad para mitigar estos riesgos.

¿Cuáles son los vectores de ataque más usados por los ciberdelincuentes?

En términos generales, la IA puede utilizarse para llevar a cabo una amplia gama de ataques informáticos, dependiendo de la habilidad del ciber atacante y del contexto en el que se esté utilizando la IA.

Algunos de los vectores de ataque más comunes son:

Recuperado de: https://assets.retarus.com/

Ataques de phishing: En estos ataques, el ciber delincuente utiliza técnicas de IA para crear mensajes de correo electrónico o sitios web de phishing que parecen legítimos, lo que permite obtener información confidencial de los usuarios. Según un informe de la consultora Accenture, el uso de IA en los ataques de phishing ha aumentado en un 400% en los últimos años[3].

Ataques de fuerza bruta: La IA también puede utilizarse para aumentar la eficacia de los ataques de fuerza bruta, en los que se intentan todas las combinaciones posibles de contraseñas hasta encontrar la correcta. Según un estudio de la firma de seguridad Imperva, el 94% de los ataques de fuerza bruta utilizan bots automatizados[4].

Ataques de botnets: Las botnets son redes de dispositivos infectados por malware que pueden ser controlados de forma remota para llevar a cabo una variedad de ataques, como el envío de spam o la realización de ataques de denegación de servicio distribuido (DDoS). Según un informe de la empresa de seguridad en línea Akamai, el 85% de los ataques DDoS son realizados por botnets[5].

Recuperado de: https://www.freepik.es/

¿Cómo hacer uso de la IA en un contexto organizacional para reducir la exposición al riesgo?

- Teniendo presente que la IA se construye a partir del desarrollo de algoritmos y técnicas computacionales capaces de imitar la inteligencia humana mediante procesos de aprendizaje automático, en problemas relacionados con **fraude**, la IA puede ser utilizada para aprender y desarrollar mecanismos de defensa contra tendencias o vectores de ataque, puesto que los sistemas de inteligencia artificial pueden analizar grandes cantidades de datos y detectar patrones sospechosos que podrían indicar la presencia de fraude o amenazas a la ciberseguridad.
- Con relación a la **Privacidad de los datos**, la inteligencia artificial requiere grandes cantidades de datos para correcto funcionamiento, en este sentido, las organizaciones necesitan asegurarse de que están cumpliendo con las regulaciones de privacidad de datos y que están tomando medidas para proteger la privacidad de sus clientes, empleados y partes interesadas.
- La inteligencia artificial plantea importantes cuestiones éticas y sociales. En este sentido, las organizaciones necesitan asegurarse de que están utilizando la inteligencia artificial de manera **ética y responsable**, y que no están perpetuando sesgos, discriminación o uso indebido.

[3] Accenture. (2021). Cyber Threatscape Report 2021. Accenture. Recuperado de https://www.accenture.com/_acnmedia/pdf-147/accenture-cyber-threatscape-report-2021.pdf#zoom=50
[4] Imperva. (2020). Bad Bot Report 2020. Imperva. Recuperado de https://www.imperva.com/resources/reports/2020-bad-bot-report/
[5] Akamai. (2020). State of the Internet/Security: Attack Spotlight Q1 2020. Akamai. Recuperado de https://www.akamai.com/content/dam/akamai/uk/documents/reports/akamai-state-of-the-internet-security-attack-spotlight-q1-2020.pdf

- La inteligencia artificial también está siendo utilizada en la robótica y la automatización de procesos. Por tal motivo, las organizaciones necesitan asegurarse de que están implementando sistemas de seguridad adecuados para proteger a los trabajadores y prevenir accidentes. Además, las organizaciones necesitan prepararse para la posibilidad de una mayor automatización en el futuro, y asegurarse de que están tomando medidas para mitigar cualquier impacto negativo en la fuerza laboral.

La inteligencia artificial tiene un gran potencial para mejorar la eficiencia y la ciberseguridad en las organizaciones, pero también plantea importantes desafíos para términos de esta disciplina del conocimiento. Las organizaciones deben implementar medidas adecuadas para proteger sus datos y sistemas contra posibles ataques y garantizar que están utilizando la inteligencia artificial de manera ética y responsable. En resumen, la inteligencia artificial es una herramienta poderosa que puede mejorar significativamente las operaciones de las organizaciones, pero su implementación debe ser cuidadosamente gestionada para evitar riesgos y asegurar que los beneficios superen los desafíos.

Tips para hacer buen uso de la IA en la vida personal y en un espacio organizacional

1. Comprender los límites de la IA: Aunque la IA puede realizar tareas complejas, aún no puede reemplazar completamente la inteligencia y habilidades humanas.
2. Conocer los beneficios de la IA: La IA puede ser muy útil para mejorar la eficiencia y la seguridad en las organizaciones, así como para simplificar tareas en la vida personal.
3. Validar fuentes confiables brindadas por la IA: Asegurarse de que la información obtenida de la IA proviene de fuentes confiables y seguras.
4. Proteger la privacidad de los datos: Asegurarse de que los datos personales no sean compartidos o utilizados de manera inapropiada.
5. Entender las implicaciones éticas: Comprender los posibles sesgos y discriminaciones que pueden ser perpetuados por la IA, y tomar medidas para evitarlos.
6. Aprender sobre la tecnología: Aprender sobre la tecnología detrás de la IA y cómo funciona puede ayudar a tomar decisiones informadas.
7. Establecer expectativas realistas: Reconocer las limitaciones de la IA y tener expectativas realistas sobre su capacidad para realizar ciertas tareas.
8. Buscar asesoramiento profesional: En un entorno organizacional, buscar asesoramiento profesional para implementar y utilizar la IA de manera efectiva.
9. Mantener la comunicación abierta: En un entorno organizacional, mantener la comunicación abierta con los empleados sobre la implementación y uso de la IA.
10. Estar preparado para cambios: En un entorno organizacional, estar preparado para posibles cambios en la fuerza laboral y tomar medidas para mitigar cualquier impacto negativo.

Canales de comunicación

El CIP CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- **Correo**: csirt@unad.edu.co
- **Twitter**: @csirtunad
- **Página web**: https://csirt.unad.edu.co

Bibliografía Propuesta

[1] McAfee. (2020). McAfee uncovers major increase in use of external attacks and collaboration by cyber criminals. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-threats-evolving-mcafee.pdf

[2] Accenture. (2021). State of cyber resilience 2021: Enhancing cyber resilience through AI and automation. https://www.accenture.com/_acnmedia/pdf-149/accenture-state-of-cyber-resilience-2021.pdf#zoom=50

[3] Accenture. (2021). Cyber Threatscape Report 2021. Accenture. Recuperado de https://www.accenture.com/_acnmedia/pdf-147/accenture-cyber-threatscape-report-2021.pdf#zoom=50

[4] Imperva. (2020). Bad Bot Report 2020. Imperva. Recuperado de https://www.imperva.com/resources/reports/2020-bad-bot-report/

[5] Akamai. (2020). State of the Internet/Security: Attack Spotlight Q1 2020. Akamai. Recuperado de https://www.akamai.com/content/dam/akamai/uk/documents/reports/akamai-state-of-the-internet-security-attack-spotlight-q1-2020.pdf