UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

EL PAPEL DE LA INTELIGENCIA ARTIFICIAL EN LA INTELIGENCIA DE AMENAZAS Y DEFENSA CIBERNÉTICA

AUTOR:

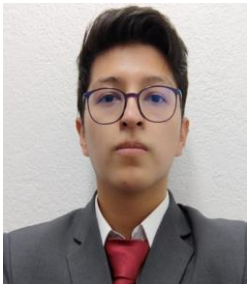
DANNY MAURICIO TOCTAGUANO VINCES

DIRECTOR:

RODOLFO XAVIER BOJORQUE CHASI

CUENCA – ECUADOR
2025

Autor:



Danny Mauricio Toctaguano Vinces
Ingeniero en Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
toctaguano.7danny@gmail.com

Dirigido por:

Rodolfo Xavier Bojorque Chasi
Ingeniero en Sistemas.
Doctor en Ciencias y Tecnologías de la Computación para Smart Cities.
rbojorque@ups.edu.ec

DEDICATORIA

Quiero dedicar esta tesis con todo mi cariño a las personas que han sido mi apoyo, mi inspiración y mi motivación constante durante todo este camino, tanto académico como personal.

Primero, a mis padres queridos. Gracias a ellos, con su amor incondicional, sacrificios y esfuerzo diario, he aprendido los valores y la fuerza que necesitaba para cumplir mis sueños. Su ejemplo de perseverancia y dedicación ha sido mi guía en los momentos difíciles y ha llenado de alegría mis días, impulsándome a seguir adelante. Gracias por creer siempre en mí, por sus palabras de aliento y por su apoyo sin límites, sin ustedes esta meta no habría sido posible.

A mis hermanos, gracias por compartir tantos momentos y por ser una fuente constante de alegría y respaldo. Su compañía ha hecho que este camino sea más llevadero y menos solitario. Cada logro en esta tesis lleva un pedacito de ustedes, porque su cariño y apoyo me han dado la motivación para continuar.

A mi abuela paterna, ese ser tan especial que con su ternura y sabiduría ha dejado una marca imborrable en mi vida. Gracias por enseñarme el valor de la paciencia, la humildad y el amor familiar.

También quiero dedicar este logro con un sentimiento profundo de gratitud y amor a mis dos abuelos maternos que ya no se encuentran con nosotros. Aunque físicamente no estén aquí, su recuerdo vive en mi corazón y en cada paso que doy.

Esta tesis es para ustedes, mi familia, porque en ella está reflejado todo su amor, apoyo y enseñanzas. Gracias por ser mi pilar y por acompañarme siempre, por estar en cada pensamiento y en cada logro.

AGRADECIMIENTO

Antes que nada, quiero agradecer de corazón a mi familia, en especial a mis padres, mi pilar más fuerte. Su amor, paciencia y apoyo constante me han impulsado a seguir adelante aun en los momentos más difíciles. Gracias por creer en mí y brindarme las herramientas para alcanzar mis metas.

Quiero dar un agradecimiento muy especial a mi tutor de tesis, el Ing. Rodolfo Bojorque, por su guía experta, su gran paciencia y su compromiso con mi crecimiento académico. Sus observaciones constructivas y el tiempo que me dedicó enriquecieron muchísimo mi trabajo y me ayudaron a profundizar en este tema.

También valoro mucho a todos los profesores que formaron parte de mi formación durante esta maestría. Su dedicación, pasión por la enseñanza y compromiso con la excelencia académica fueron fundamentales para que pudiera adquirir los conocimientos y las habilidades necesarias para completar esta etapa.

Tabla de Contenido

El Papel de la Inteligencia Artificial en la Inteligencia de Amenazas y Defensa Cibernética

Autor(es):

Danny Mauricio Toctaguano Vinces

Resumen

La inteligencia artificial (IA) se ha convertido en una pieza clave para la defensa cibernética y la inteligencia de amenazas. Gracias a esta tecnología, las organizaciones tienen una forma mucho más efectiva de anticiparse, detectar y responder a ataques que son cada vez más complejos y cambiantes. Diversos estudios recientes muestran que la IA es capaz de identificar rápidamente comportamientos extraños y amenazas emergentes que los sistemas tradicionales, basados en firmas, no captan. Además, las herramientas basadas en IA reducen la cantidad de falsas alarmas, que suelen agobiar a los equipos de seguridad, permitiendo que se enfoquen en las alertas verdaderamente importantes y respondan de forma más eficiente.

Sin embargo, usar IA también plantea retos importantes. Entre ellos están los sesgos en los algoritmos, la necesidad de que los modelos sean transparentes y entendibles, la protección de la privacidad, la responsabilidad en decisiones automáticas y el riesgo de que la IA misma sea usada con fines maliciosos. Además, a nivel técnico, todavía hay que lidiar con la calidad de los datos, posibles ataques dirigidos a confundir los sistemas, falsos positivos o negativos que no desaparecen totalmente, y evitar depender demasiado de la tecnología sin mantener el control humano.

En general, la inteligencia artificial es una herramienta imprescindible para una ciberseguridad moderna. Gracias a ella, es posible anticipar, detectar y responder mejor a las amenazas, elevando así los estándares de protección en un mundo digital que cada vez está más interconectado y es más desafiante.

Palabras clave:
Inteligencia Artificial, Seguridad Cibernética, Defensa Cibernética, Prevención de Ataques, Inteligencia de Amenazas.

Abstract

Artificial intelligence (AI) has become a key piece for cybersecurity and threat intelligence. Thanks to this technology, organizations have a much more effective way to anticipate, detect, and respond to increasingly complex and changing attacks. Various recent studies show that AI is capable of quickly identifying unusual behaviors and emerging threats that traditional signature-based systems do not capture. Moreover, AI-based tools reduce the number of false alarms, which often overwhelm security teams, allowing them to focus on truly important alerts and respond more efficiently.

However, using AI also poses significant challenges. Among them are biases in algorithms, the need for models to be transparent and understandable, the protection of privacy, accountability in automatic decisions, and the risk that AI itself could be used for malicious purposes. Furthermore, at a technical level, there are still issues to deal with regarding data quality, potential attacks aimed at confusing the systems, persistent false positives or negatives, and avoiding overreliance on technology without maintaining human control.

In general, artificial intelligence is an essential tool for modern cybersecurity. Thanks to it, it is possible to anticipate, detect, and respond better to threats, thus raising the standards of protection in an increasingly interconnected and challenging digital world.

key words:
Artificial Intelligence, Cyber Security, Cyber Defense, Attack Prevention, Threat Intelligence.

1. Introducción

La evolución de las amenazas cibernéticas ha sido notable en las últimas décadas, pasando de ataques perpetrados por individuos en busca de notoriedad a operaciones sofisticadas orquestadas por actores estatales, grupos criminales y hackers altamente capacitados. Según el informe de Verizon 2023 [1] sobre investigaciones de violaciones de datos, los incidentes de seguridad cibernética han aumentado exponencialmente, afectando tanto a empresas como a gobiernos. Este incremento en el volumen y la complejidad de las amenazas ha superado la capacidad de las soluciones tradicionales de ciberseguridad para detectarlas y mitigarlas efectivamente, lo que ha impulsado la adopción de tecnologías avanzadas como la Inteligencia Artificial (IA) [2,3].

La IA ha transformado diversos sectores, y su integración en la inteligencia de amenazas se ha vuelto crucial en un entorno donde las amenazas cibernéticas son cada vez más sofisticadas. La inteligencia de amenazas cibernéticas (CTI) implica la recopilación, análisis y aplicación de información sobre amenazas potenciales para prevenir ataques o mitigar sus efectos. [4,5]. Esta inteligencia se clasifica en tres categorías: táctica, operativa y estratégica, cada una con enfoques y aplicaciones distintas en la defensa cibernética [6,7]. Tradicionalmente, este proceso se basaba en el análisis manual de datos, lo que resulta ineficiente frente al volumen actual de ataques.

La IA permite automatizar el análisis de grandes volúmenes de datos, identificando patrones y anomalías que podrían representar amenazas [4,5]. Esto no solo mejora la eficacia en la detección de amenazas, sino que también optimiza los recursos humanos al reducir el tiempo dedicado a tareas repetitivas. La defensa cibernética se centra en proteger redes, sistemas y datos contra ataques y accesos no autorizados. Con un aumento en los vectores de ataque como ransomware, phishing avanzado y ataques de día cero, la IA está revolucionando cómo las organizaciones detectan y responden a estos eventos.

Las soluciones basadas en IA [8] pueden identificar y bloquear amenazas en tiempo real, aprendiendo continuamente de los datos para adaptarse a nuevas tácticas utilizadas por los atacantes. La implementación de IA no solo mejora la eficiencia operativa al automatizar tareas repetitivas, sino que también reduce costos asociados con brechas de seguridad. Además, los modelos basados en IA son adaptativos y pueden aprender y ajustarse a nuevas amenazas a medida que emergen.

Por último, la adopción proactiva de soluciones basadas en IA no solo ayuda a mitigar riesgos derivados de violaciones de seguridad, sino que también protege la parte económica y reputacional de una organización. En un panorama digital cada vez más complejo y amenazante, la integración efectiva de la Inteligencia Artificial en la inteligencia sobre amenazas cibernéticas es esencial para abordar los desafíos actuales que enfrentan las organizaciones.

2. Determinación del Problema

La ciberseguridad se ha convertido en una de las principales preocupaciones para organizaciones de todos los sectores en un mundo cada vez más digitalizado. Con el aumento exponencial de las amenazas cibernéticas, que van desde ataques de ransomware hasta violaciones de datos masivos, las organizaciones enfrentan desafíos significativos para proteger su infraestructura y datos sensibles. En este contexto, la Inteligencia Artificial (IA) emerge como una herramienta prometedora que podría revolucionar la inteligencia sobre amenazas y mejorar la defensa cibernética. [9, 10] Sin embargo, la integración efectiva de técnicas avanzadas de IA en los procesos de inteligencia de amenazas presenta diversas dificultades como la falta de integración efectiva de técnicas avanzadas de Inteligencia Artificial en los procesos de inteligencia de amenazas cibernéticas, esto limita la capacidad de las organizaciones para detectar y responder a incidentes de manera eficiente.

Las soluciones tradicionales están basadas en firmas, los cuales son ineficientes para identificar amenazas desconocidas o nuevas tácticas utilizadas por los atacantes. La detección manual, que a menudo depende del análisis humano, es propensa a errores y puede resultar en tiempos prolongados para identificar incidentes críticos. Adicional, la velocidad con la que se producen los ataques cibernéticos requiere respuestas rápidas que muchas organizaciones no pueden proporcionar con sus sistemas actuales. La falta de automatización en los procesos de respuesta a incidentes no solo retrasa la mitigación del daño, sino que también genera un elevado número de falsos positivos, lo que sobrecarga a los equipos de seguridad y desvía recursos esenciales. [9, 11] La incapacidad para filtrar adecuadamente las alertas puede resultar en la pérdida de tiempo valioso en la respuesta a incidentes reales, lo que puede tener consecuencias devastadoras.

Este proyecto tiene como fin investigar cómo las técnicas avanzadas de IA pueden ser aplicadas efectivamente en el ámbito de la inteligencia sobre amenazas

cibernéticas y como puede mejorar las capacidades defensivas ante incidentes cibernéticos [11].

3. Marco teórico referencial

3.1 Inteligencia Artificial.

La Inteligencia Artificial (IA) es una disciplina dentro de las ciencias de la computación que se centra en la creación de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Estas tareas incluyen el aprendizaje, el razonamiento, la percepción y la toma de decisiones. La IA busca emular las capacidades cognitivas humanas, permitiendo que las máquinas realicen funciones complejas a través de algoritmos y modelos computacionales. El término fue acuñado por John McCarthy en 1956 durante la Conferencia de Dartmouth, donde se establecieron las bases para el desarrollo de esta área de estudio [12].

A lo largo del tiempo, la IA ha evolucionado y se ha diversificado en múltiples subcampos, cada uno enfocado en diferentes aspectos del comportamiento inteligente. Entre estos subcampos se encuentran el aprendizaje automático, el procesamiento del lenguaje natural y la visión por computadora. La IA no solo se limita a tareas específicas; también tiene aplicaciones en áreas como la medicina, donde se utiliza para diagnósticos asistidos por computadora, y en finanzas, para detectar fraudes y realizar análisis predictivos [13][14].

La definición de IA ha sido objeto de debate entre expertos. Stuart Russell y Peter Norvig, en su libro "Artificial Intelligence: A Modern Approach", describen la IA como el estudio de agentes que perciben su entorno y realizan acciones para alcanzar objetivos específicos [13]. Esta capacidad de adaptación y aprendizaje es fundamental para el desarrollo de sistemas inteligentes que pueden mejorar su rendimiento a medida que interactúan con su entorno.

Sin embargo, a medida que la IA avanza, también surgen preocupaciones éticas y sociales. La automatización impulsada por la IA plantea preguntas sobre el futuro del trabajo y los impactos en la sociedad. Se estima que un gran porcentaje de empleos podría ser automatizado en los próximos años, lo que requiere una

reflexión sobre cómo gestionar estos cambios [15]. Por lo tanto, es crucial abordar tanto las oportunidades como los desafíos que presenta la inteligencia artificial en el mundo actual.

3.2 Inteligencia artificial en amenazas cibernéticas

La Inteligencia Artificial (IA) ha emergido como un componente crucial en el ámbito de la ciberseguridad, actuando tanto como una herramienta defensiva como un facilitador de ataques cibernéticos. En la actualidad, los ciberdelincuentes utilizan algoritmos de IA para automatizar y personalizar sus ataques, lo que les permite adaptarse rápidamente a las defensas de sus objetivos. Esta capacidad de adaptación hace que los ataques sean más sigilosos y difíciles de detectar, representando un desafío significativo para las organizaciones que buscan proteger sus activos digitales. Según un informe, los hackers pueden emplear IA para crear correos electrónicos de phishing más convincentes y sofisticados, aumentando así la probabilidad de que los usuarios caigan en trampas digitales y revelen información sensible [16][17].

Uno de los aspectos más preocupantes del uso de IA en ciberataques es la velocidad con la que se pueden propagar. Los algoritmos de IA permiten identificar y explotar vulnerabilidades en cuestión de segundos, lo que reduce drásticamente el tiempo de reacción de las defensas cibernéticas convencionales. Esto significa que los ataques pueden escalar rápidamente, dificultando su contención y mitigación [16][18]. Además, la IA facilita la creación de malware avanzado que puede evadir sistemas de detección tradicionales al optimizarse automáticamente según las respuestas del entorno infectado [17][18].

La ingeniería social también ha evolucionado gracias a la IA. Los ciberdelincuentes ahora pueden recopilar y analizar grandes volúmenes de datos para crear perfiles detallados de sus víctimas potenciales, lo que les permite diseñar ataques más efectivos y personalizados [17]. Esta capacidad para realizar ataques dirigidos no

solo aumenta la eficacia de las campañas maliciosas, sino que también plantea serios riesgos para la privacidad y la seguridad personal.

A pesar de estos desafíos, la IA también se utiliza para fortalecer las defensas cibernéticas. Las organizaciones están implementando sistemas basados en IA para detectar amenazas avanzadas en tiempo real, analizar vulnerabilidades y responder a incidentes con mayor eficacia. Estas herramientas permiten una identificación más rápida de patrones anómalos en el tráfico de red, lo que mejora significativamente la capacidad de respuesta ante posibles ataques [16][17]. Sin embargo, es crucial equilibrar el uso de estas tecnologías con una comprensión clara de sus limitaciones y riesgos inherentes.

En conclusión, la inteligencia artificial está transformando el panorama de las amenazas cibernéticas. Si bien ofrece oportunidades significativas para mejorar la seguridad cibernética, también presenta nuevos retos que deben ser abordados con urgencia. La colaboración entre expertos en seguridad, el desarrollo responsable de tecnologías y una regulación adecuada son esenciales para mitigar los riesgos asociados con el uso malintencionado de la IA en el ámbito cibernético.

3.3 Amenazas

La ISO 27000 establece un marco normativo para la gestión de la seguridad de la información, y dentro de este contexto, el concepto de amenaza es fundamental para entender los riesgos asociados a los activos de información. Según esta norma, una amenaza se define como cualquier circunstancia o evento con el potencial de causar daño a los activos de información, lo que puede resultar en incidentes que comprometan la confidencialidad, integridad o disponibilidad de dichos activos. Este enfoque implica que las amenazas pueden ser tanto intencionales, como ataques cibernéticos, como no intencionales, como desastres naturales o fallos técnicos [19][21].

Las amenazas pueden desencadenar incidentes que alteran el estado de seguridad de los activos amenazados. Por lo tanto, es crucial para las organizaciones

identificar y evaluar estas amenazas en el contexto de un sistema de gestión de seguridad de la información (SGSI). La norma ISO 27001 enfatiza que la identificación adecuada de amenazas es un componente clave dentro del proceso de evaluación de riesgos, ya que permite a las organizaciones implementar controles adecuados para mitigar los impactos potenciales [20][22]. En este sentido, las amenazas no solo se consideran eventos aislados, sino que deben ser analizadas en relación con las vulnerabilidades existentes en los activos, ya que la coexistencia de una amenaza y una vulnerabilidad es lo que da origen a un riesgo real [20][23].

Además, la ISO 27000 destaca que las amenazas son externas a los activos de información y pueden variar en su naturaleza y alcance. Esto significa que es esencial para las organizaciones realizar un análisis continuo y dinámico del entorno en el que operan para identificar nuevas amenazas a medida que surgen. Por ejemplo, la creciente dependencia de tecnologías digitales ha introducido nuevas amenazas relacionadas con ciberseguridad, lo que obliga a las organizaciones a adaptarse y actualizar sus estrategias de seguridad [21][22]. La gestión proactiva de estas amenazas no solo ayuda a prevenir incidentes, sino que también contribuye a la resiliencia organizacional frente a posibles crisis.

En conclusión, el concepto de amenaza según la ISO 27000 es integral para la comprensión y gestión efectiva del riesgo en el ámbito de la seguridad de la información. Al identificar y evaluar las amenazas adecuadamente, las organizaciones pueden establecer medidas preventivas y reactivas que protejan sus activos críticos y aseguren su funcionamiento continuo.

3.4 Inteligencia de amenazas

La inteligencia de amenazas consiste en un proceso que implica la recopilación, el análisis y la interpretación de información relacionada con ciberamenazas presentes o potenciales que podrían afectar a una organización o sistema. No se limita únicamente a reunir datos sobre posibles ataques, sino que transforma esa

información en conocimiento útil que permite a las organizaciones anticiparse, identificar y responder con mayor eficacia a los riesgos de seguridad.[24][25][26]

Este procedimiento abarca la detección de vulnerabilidades, así como las tácticas, técnicas y procedimientos (TTP) que emplean los atacantes, además de los indicadores de compromiso (IOC) que facilitan la identificación de patrones y comportamientos maliciosos. La inteligencia de amenazas ayuda a clasificar los riesgos según su nivel de gravedad y relevancia, lo que favorece la toma de decisiones fundamentadas para reforzar las defensas y mitigar el impacto de los ciberataques.[26][28]

Asimismo, esta inteligencia promueve un enfoque proactivo en ciberseguridad, pasando de una reacción a los incidentes a una anticipación basada en análisis detallados y datos precisos. Esto contribuye a acelerar la detección y respuesta, reducir los costos asociados a las brechas de seguridad y garantizar el cumplimiento de las normativas vigentes.[25][27]

3.5 Ciberseguridad

La ciberseguridad se define como el conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos contra amenazas cibernéticas. Su objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de la información digital, asegurando que los datos y los sistemas estén protegidos de accesos no autorizados y ataques maliciosos. En un mundo cada vez más interconectado, donde las organizaciones dependen de la tecnología para llevar a cabo sus operaciones diarias, la ciberseguridad se ha convertido en un componente esencial para prevenir riesgos asociados con la manipulación no autorizada de datos, interrupciones del sistema y violaciones de la privacidad [29].

La ciberseguridad abarca una amplia gama de medidas que incluyen la protección de hardware, software y redes. Esto implica no solo la implementación de tecnologías avanzadas como firewalls y software antivirus, sino también el establecimiento de políticas y procedimientos que regulen el uso seguro de los

recursos tecnológicos. Las organizaciones deben adoptar un enfoque integral que combine personas, procesos y tecnologías para crear un entorno seguro. Esto incluye la capacitación del personal en prácticas seguras, así como la realización de auditorías regulares para identificar vulnerabilidades [30].

Además, es importante destacar que la ciberseguridad no es un estado absoluto; siempre existe un riesgo residual que debe ser gestionado. Esto significa que, aunque se implementen medidas de seguridad robustas, nunca se puede garantizar una protección del 100%. Por lo tanto, las organizaciones deben estar preparadas para responder a incidentes de seguridad y tener planes de recuperación ante desastres en su lugar [31]. La creciente sofisticación de los ciberataques, como el ransomware y el phishing, subraya la necesidad de mantener una vigilancia constante y actualizar las estrategias de seguridad para adaptarse a nuevas amenazas [32].

La ciberseguridad es una disciplina crítica que juega un papel fundamental en la protección de los activos digitales de las organizaciones. A medida que el panorama de amenazas continúa evolucionando, es imperativo que las empresas implementen soluciones efectivas y mantengan una cultura organizacional centrada en la seguridad para mitigar los riesgos asociados con el ciberespacio [33].

4. Materiales y metodología

El presente trabajo se fundamenta en una revisión sistemática de literatura científica, orientada a analizar el impacto de las técnicas de Inteligencia Artificial (IA) en la inteligencia de amenazas y la defensa cibernética. Se emplea como marco metodológico el protocolo PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), que permite garantizar la transparencia y replicabilidad del proceso de revisión.

4.1 Fuentes de información

La recolección de datos secundarios se llevó a cabo mediante búsquedas en los principales repositorios y bases de datos científicas especializadas, tales como:

- IEEE Xplore
- Scopus
- Google Scholar
- ScienceDirect
- SpringerLink

Los criterios de inclusión consideran publicaciones entre 2018 y 2024, artículos con revisión por pares, informes técnicos y estudios de caso aplicados a IA y ciberseguridad. Se utilizaron combinaciones booleanas de palabras clave como "artificial intelligence", "cyber threat intelligence", "machine learning for cybersecurity", "anomaly detection", entre otras.

4.2 Proceso de selección

La revisión se realizó en cuatro fases:

- Identificación: recuperación de literatura mediante términos de búsqueda definidos.
- Filtrado: eliminación de duplicados y artículos no relacionados.

- Evaluación de elegibilidad: análisis del resumen y los objetivos de cada estudio.
- Inclusión: selección final de documentos relevantes para el análisis cualitativo.

4.3 Herramientas de análisis

Para apoyar la exploración eficiente de la literatura, se utilizó software con capacidades de procesamiento de lenguaje natural (NLP) e indexación semántica asistida por IA, lo cual permitió mejorar la precisión en la selección de fuentes relevantes. Además, se emplearon técnicas de análisis temático para clasificar los hallazgos en categorías como: detección automatizada de amenazas, respuesta a incidentes, explicabilidad de modelos, y limitaciones operativas.

4.4 Resultados esperados

Se espera que esta revisión sistemática permita:

- Identificar las técnicas de IA más utilizadas en inteligencia de amenazas cibernéticas.
- Determinar los beneficios operativos que estas técnicas aportan (ej. reducción de tiempos de detección, disminución de falsos positivos).
- Evidenciar las limitaciones y desafíos técnicos, éticos y organizacionales asociados con su implementación.
- Proponer recomendaciones basadas en evidencia para una integración efectiva de IA en los procesos de defensa cibernética.

La sistematización de estos hallazgos proporcionará un marco referencial sólido que podrá ser utilizado por organizaciones públicas o privadas interesadas en fortalecer su postura de ciberseguridad mediante tecnologías basadas en inteligencia artificial.

4.5 Técnicas de inteligencia artificial (IA) aplicadas en la inteligencia de amenazas

Actualmente la inteligencia artificial (IA) se han convertido en aliada clave para protegernos de las amenazas digitales. Herramientas como el aprendizaje automático, el aprendizaje profundo, la inteligencia artificial generativa y el análisis predictivo están transformando la forma en que detectamos y prevenimos ciberataques.

Estas tecnologías nos permiten procesar enormes cantidades de información en tiempo real, reconocer comportamientos extraños y, lo más importante, adelantarnos a los ataques antes de que ocurran. Esto es vital porque los ciberataques son cada vez más sofisticados y difíciles de detectar [34][36][37].

4.5.1. Aprendizaje automático y aprendizaje profundo

El aprendizaje automático y el aprendizaje profundo se utiliza actualmente para analizar cómo se comporta el tráfico en la red, las acciones de los usuarios y los eventos de seguridad. Así, pueden identificar amenazas desconocidas o de día cero sin depender exclusivamente de firmas tradicionales [37][38]. La inteligencia artificial generativa también puede ser utilizada para generar datos sintéticos que mejoran la formación de los equipos de seguridad y hacen que los sistemas de detección sean más precisos [35][36].

4.5.2. Análisis predictivo

El análisis predictivo basado en IA permite anticipar tendencias en los ataques y detectar indicios tempranos de compromisos, automatizando respuestas inmediatas para neutralizar amenazas como malware o intentos de phishing, incluso sin que una persona tenga que intervenir [34][36].

5.1.3. Procesamiento de lenguaje natural

El procesamiento de lenguaje natural ayuda a simplificar y resumir informes complejos de inteligencia, facilitando que los analistas tomen decisiones rápidas y bien fundamentadas [36].

Todas estas técnicas funcionan mejor cuando se combinan con modelos modernos de seguridad, como el enfoque de confianza cero (Zero Trust), que exige verificar constantemente quién accede a qué, dificultando que los atacantes se muevan dentro de la red [34]. Sin embargo, se reconoce que la IA debe complementarse con la experiencia humana, esto para mitigar riesgos como alucinaciones de modelos o degradación en la calidad de las detecciones, buscando un equilibrio óptimo entre automatización y supervisión humana [36].

4.6 Herramientas de Ciberseguridad que utilizan algoritmos de IA

Hoy en día, cuando las amenazas cibernéticas son cada vez más complejas y difíciles de detectar, contar con herramientas que utilizan inteligencia artificial (IA) se ha vuelto esencial para fortalecer la inteligencia de amenazas y la defensa cibernética. Estas tecnologías no solo ayudan a identificar peligros con mayor rapidez, sino que también fortalece la capacidad de anticiparse y responder eficazmente a los ataques.

4.6.1. CrowdStrike Falcon

es una plataforma en la nube que protege los dispositivos conectados usando inteligencia artificial para analizar millones de eventos cada día. Gracias a su motor llamado Charlotte AI, entrenado con millones de decisiones globales, puede identificar rápidamente cuáles alertas son amenazas reales y cuáles son falsas alarmas, reduciendo enormemente el tiempo que los equipos de seguridad dedican a revisar cada alerta. Lo mejor es que esta tecnología trabaja de forma autónoma, pero siempre bajo el control y supervisión de los expertos, quienes pueden enfocarse en los incidentes más críticos sin perder el control de las acciones automatizadas [39][40][41].

4.6.2. Fortinet con FortiEDR y FortiAI

Ofrece protección en tiempo real contra ataques complejos. Estas herramientas permiten una vigilancia constante, detectan amenazas de forma proactiva y automatizan las respuestas, ayudando tanto a los equipos de seguridad como a los encargados de las redes. Además, su laboratorio de inteligencia, FortiGuard Labs, ha sido pionero en aplicar IA para analizar comportamientos y generar información valiosa sobre amenazas [42].

4.6.3. IBM Security QRadar

Esta plataforma utiliza inteligencia artificial y aprendizaje automático para detectar patrones sospechosos y relacionar eventos de seguridad en infraestructuras complejas. Esto acelera la investigación de incidentes, automatiza la detección de anomalías y prioriza los casos más urgentes, ayudando a responder más rápido y con mayor eficacia. QRadar es muy popular en América Latina y puede reducir hasta un 90% el tiempo dedicado a investigar incidentes [41][43].

4.6.4. Vectra AI

Se especializa en detectar y responder a ciberataques analizando constantemente el tráfico de red, el comportamiento de los usuarios y los entornos en la nube. Utiliza IA para identificar tanto amenazas conocidas como señales sutiles de ataques avanzados, y destaca por su capacidad para priorizar automáticamente las amenazas según su gravedad, lo que mejora la rapidez y efectividad de la respuesta [44][45][46].

4.6.5. Check Point Infinity

Esta herramienta combina la inteligencia artificial con la flexibilidad de la nube para ofrecer una protección completa en tiempo real. Usa más de cincuenta motores de IA para detener ataques sofisticados como malware de día cero, phishing y ataques al DNS. Infinity AI unifica la gestión de seguridad y automatiza la respuesta a

incidentes, integrando inteligencia de amenazas en todos los entornos tecnológicos [47].

4.6.6. Splunk

Emplea IA para monitorear en tiempo real, analizar registros y detectar anomalías en infraestructuras digitales. Su enfoque combina la experiencia humana con la inteligencia artificial para construir Centros de Operaciones de Seguridad (SOC) integrados, capaces de responder a amenazas emergentes y ataques impulsados por IA. Splunk ayuda a automatizar tareas críticas y mejora la visibilidad y la respuesta ante incidentes [41][48].

Además, la combinación de estas herramientas con el modelo de seguridad Zero Trust potencia la defensa cibernética al exigir verificación continua y controles estrictos de acceso, mitigando riesgos tanto internos como externos y fortaleciendo la resiliencia organizacional.

4.7 Ventajas de la IA en la detección de amenazas

La inteligencia artificial (IA) está cambiando por completo la ciberseguridad, haciéndola mucho más eficiente y proactiva, ya que la IA nos ayuda a defendernos mejor de los ataques y a reaccionar más rápido cuando algo malo sucede.

4.7.1. Rapidez y precisión ante los ataques:

La IA permite analizar grandes volúmenes de datos e información en tiempo real, detectando anomalías con una velocidad y precisión que superan ampliamente las capacidades humanas. Esto significa que podemos identificar posibles ataques antes de que causen un desastre. Esto permite identificar posibles ataques antes de que causen daños graves y actuar rápidamente, automatizando tareas como aislar dispositivos infectados o eliminar malware, lo que reduce muchísimo el tiempo de reacción y el daño que un ataque podría provocar [49][50][53].

4.7.2. Menos falsas alarmas y equipos más eficientes:

Los algoritmos de aprendizaje están constantemente aprendiendo y mejorando, distinguiendo con mucha más precisión entre lo que es un comportamiento normal y lo que es realmente una amenaza. Así, los equipos de seguridad reciben menos notificaciones innecesarias y pueden concentrarse en lo que de verdad importa, esto optimiza los recursos y hace que el trabajo sea mucho más efectivo [52][53]. Si a esto le sumamos el enfoque de seguridad "Zero Trust" (donde no se confía en nadie y todo se verifica), la IA mejora aún más la visibilidad y nos permite ajustar las políticas de seguridad de forma dinámica para mitigar las amenazas de forma más precisa [51].

4.7.3. Automatización para un SOC más inteligente:

La IA facilita la automatización de muchas tareas en los Centros de Operaciones de Seguridad (SOC), integrando herramientas y datos para acelerar la investigación y resolución de incidentes. Esta automatización no solo hace que todo funcione mejor, sino que también ayuda a los analistas a tomar decisiones más rápidas y acertadas, dándoles resúmenes inteligentes y contextualizando las alertas complejas [52][54]. Sin embargo, es importante destacar que la experiencia humana sigue siendo clave para supervisar y validar estas acciones automatizadas, asegurando un balance adecuado entre la tecnología y el criterio experto [52].

4.8 Desafíos éticos y técnicos en el uso de IA

La inteligencia artificial (IA) ha traído grandes avances en la detección y defensa contra amenazas cibernéticas, pero también presenta desafíos importantes que debemos enfrentar para asegurar que su uso sea efectivo, justo y confiable.

4.8.1. Retos Éticos

Sesgos y discriminación:

Los sistemas de IA aprenden a partir de datos que son proporcionados para su entrenamiento, y si esos datos son erróneos o de mala calidad, las decisiones que tome la IA pueden ser injustas o inexactas. Esto es especialmente delicado cuando hablamos de proteger a personas o comunidades diversas, donde la equidad debe ser una prioridad.

Falta de transparencia:

Muchas veces, las decisiones que toma la IA son difíciles de entender o explicar, lo que genera desconfianza y complica la supervisión. Es fundamental que los usuarios y responsables puedan comprender cómo y por qué la IA actúa de determinada manera.

Privacidad y protección de datos:

Para funcionar bien, la IA necesita procesar grandes cantidades de información, lo que puede poner en riesgo la privacidad de personas y organizaciones si no se manejan adecuadamente los datos, con políticas claras de protección y anonimización.

Responsabilidad:

Determinar quién es responsable ante errores, daños o decisiones erróneas tomadas por sistemas autónomos de IA es un reto, especialmente en incidentes críticos de ciberseguridad.

Uso indebido de la IA:

La misma tecnología que ayuda a defendernos puede ser usada por los atacantes para crear amenazas más sofisticadas, como falsificaciones digitales (deepfakes), campañas de phishing automatizadas o malware difícil de detectar.

4.8.2. Retos Técnicos

Calidad de los datos:

La efectividad de la IA depende mucho de la calidad y variedad de los datos con los que se entrena. Si esos datos son incompletos o sesgados, la IA puede fallar al detectar nuevas amenazas.

Ataques contra la IA:

Los ciberdelincuentes pueden intentar engañar a los sistemas de IA manipulando los datos que reciben, para evitar ser detectados o causar daños.

Falsas alarmas y omisiones:

Aunque la IA ayuda a reducir las falsas alertas, todavía puede generar notificaciones innecesarias o pasar por alto amenazas reales, lo que puede saturar a los equipos de seguridad o dejar vulnerabilidades abiertas.

Dependencia tecnológica:

Confiar demasiado en la IA puede ser un riesgo si estos sistemas fallan o son atacados, especialmente en infraestructuras críticas donde la seguridad es vital.

Actualización constante:

Las amenazas evolucionan rápidamente, por lo que los modelos de IA deben estar en constante actualización y mejora para seguir siendo efectivos.

4.8.3. Propuestas de Solución

Para superar los desafíos que trae el uso de la inteligencia artificial (IA) en la detección de amenazas y la defensa cibernética, es fundamental adoptar un conjunto de soluciones integrales que aseguren un desarrollo responsable, transparente y efectivo de estas tecnologías.

Contar con códigos éticos y regulaciones específicas que guíen el diseño y uso de sistemas de IA en ciberseguridad:

Normativas como las “Ethics Guidelines for Trustworthy AI” de la Comisión Europea promueven valores esenciales como la transparencia, la igualdad, la responsabilidad y la protección de la privacidad. Estos estándares ayudan a que desarrolladores y organizaciones actúen de manera justa y rindan cuentas por las decisiones automatizadas, generando confianza en el uso de la IA [55][56].

Realizar auditorías periódicas a los algoritmos

Esto es clave para detectar y corregir sesgos que puedan existir en los modelos de IA. Estas revisiones, que idealmente incluyen expertos independientes, permiten evaluar tanto el desempeño técnico como ético de los sistemas, asegurando que no se perpetúen desigualdades o errores discriminatorios. Además, la auditoría fomenta la mejora continua y la adaptación de los algoritmos a diferentes contextos y cambios [55][57].

Asegurar que los datos usados para entrenar la IA sean de alta calidad, representativos y seguros:

Esto implica cuidar cuidadosamente los conjuntos de datos, anonimizar la información y cumplir con leyes de protección de datos como el GDPR. También es importante implementar técnicas que protejan los sistemas contra ataques diseñados para engañar a la IA y manipular sus resultados [57][58].

Mantener siempre planes de contingencia y supervisión humana:

La combinación de inteligencia artificial con la experiencia humana permite validar alertas, corregir errores y tomar decisiones éticas en situaciones complejas, asegurando respuestas más seguras y equilibradas [57][59].

Establecer mecanismos claros de responsabilidad

Esto permite definir quién responde cuando la IA comete errores o causa daños, para esto se requiere desarrollar marcos legales y políticas internas que regulen el uso de estas tecnologías, garantizando transparencia, justicia y protección de los derechos fundamentales [59][60].

4.9 IA vs. Analistas Humanos en Respuesta a Incidentes y Reducción de Falsos Positivos

La tabla 1 compara cómo la inteligencia artificial (IA) y los analistas humanos abordan la respuesta a incidentes y la reducción de falsos positivos en la detección de amenazas cibernéticas.

Tabla 1: Inteligencia Artificial vs Analistas Humanos

Aspecto	IA en Ciberseguridad	Analistas Humanos en Ciberseguridad
Velocidad de respuesta	Responde en tiempo real, 24/7, sin fatiga ni pausas. Automatiza acciones inmediatas como aislamiento de sistemas o bloqueo de accesos.	Limitada por horarios, fatiga y carga de trabajo. La respuesta puede retrasarse, especialmente fuera de horario laboral.
Reducción de falsos positivos	Utiliza algoritmos avanzados para diferenciar entre amenazas reales y actividades legítimas, disminuyendo alertas innecesarias y priorizando incidentes críticos.	Puede verse sobrecargado por el volumen de alertas, lo que aumenta el riesgo de pasar por alto amenazas reales o responder a falsos positivos.
Capacidad de análisis	Analiza grandes volúmenes de datos y patrones complejos en segundos, detectando amenazas emergentes y desconocidas.	Analiza datos de forma manual, lo que limita la capacidad de procesar grandes volúmenes y puede dificultar la detección de amenazas sofisticadas.
Consistencia y precisión	Mantiene un nivel constante de precisión y calidad, sin verse afectada por el cansancio o el estrés.	La precisión puede variar según la experiencia, el estado físico y mental del analista, y la carga de trabajo.
Adaptabilidad	Aprende y se actualiza continuamente con nuevos datos y patrones de ataque, mejorando su eficacia con el tiempo.	Requiere formación y actualización constante; la adaptación a nuevas amenazas depende de la capacitación y experiencia individual.
Interpretación y contexto	Puede carecer de contexto situacional o interpretación creativa, lo que limita la	Aporta juicio crítico, creatividad y contexto organizacional, esenciales

	comprensión de amenazas complejas o novedosas.	para interpretar incidentes complejos y tomar decisiones estratégicas.
Costos y escalabilidad	Escalable y rentable para monitoreo continuo; reduce la necesidad de grandes equipos humanos.	Requiere mayor inversión en personal y formación para cubrir turnos y gestionar el aumento de incidentes.

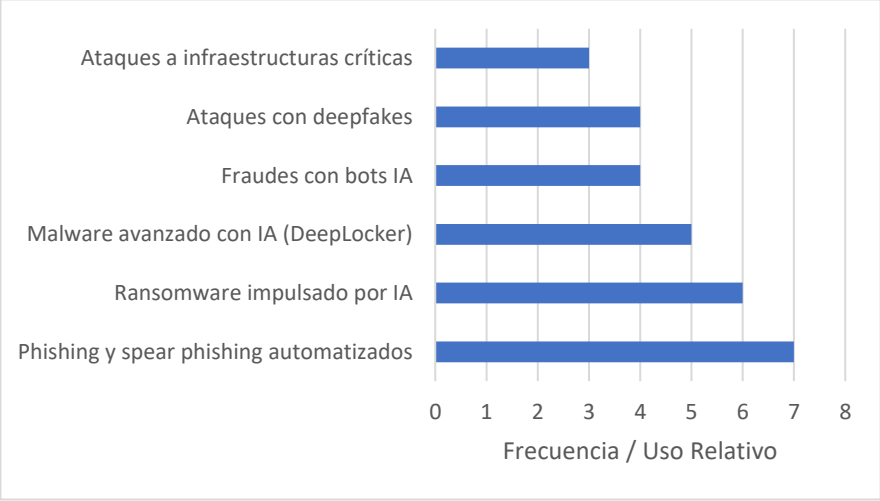
Puntos Clave

- La IA destaca en la automatización, velocidad y reducción de falsos positivos, permitiendo a los equipos de seguridad centrarse en incidentes realmente críticos y estratégicos.
- La IA no reemplaza completamente a los humanos, pero redefine su rol, liberándolos de tareas repetitivas y permitiéndoles aportar valor en áreas donde la creatividad y el juicio son esenciales.

4.10 La IA y su influencia en la ciberdelincuencia y la ciberdefensa

En los últimos tiempos, los ciberataques han crecido de manera exponencial, en gran parte gracias al uso de la inteligencia artificial. En la imagen que se presenta a continuación, se muestra la frecuencia e impacto de estos ataques en una escala del 1 al 7, donde el 7 indica la mayor incidencia.

Imagen 1: Ciberataques que utilizan IA



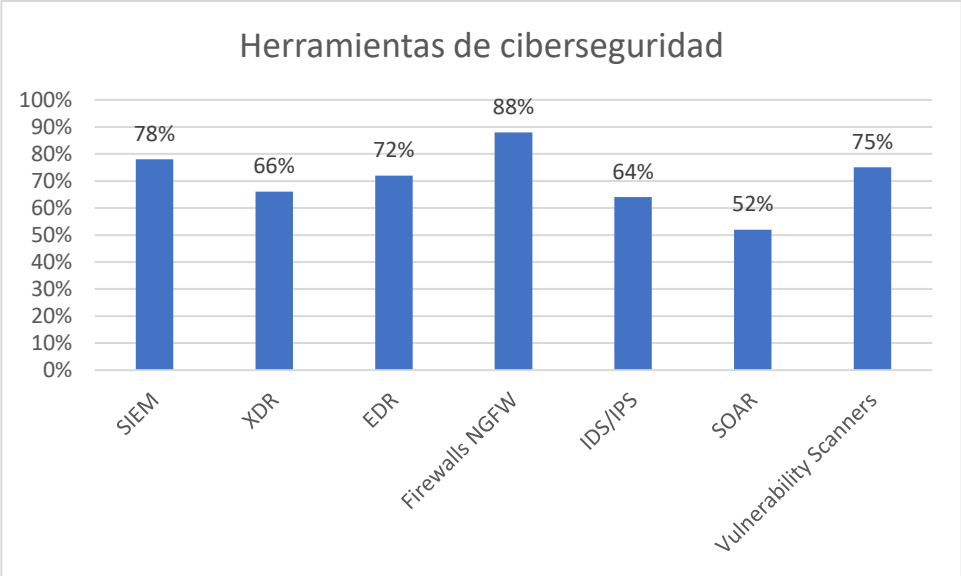
La imagen 1 expone que los ataques de tipo Phishing y Ransomware son los que más utilizan IA, siendo los más comunes y peligrosos en este campo.

El gráfico de barras anterior refleja claramente el aumento tanto en la sofisticación como la frecuencia de las amenazas cibernéticas. Ante esta situación, numerosas empresas de ciberseguridad están incorporando inteligencia artificial en sus herramientas para mejorar la detección y respuesta ante amenazas digitales. A continuación, se presentan algunas de las herramientas de seguridad que ya han integrado la IA en sus sistemas, aprovechando esta tecnología para ofrecer una protección más rápida, precisa y eficaz contra los ataques cibernéticos:

- XDR (Detección y Respuesta Extendida): Es una solución que ofrece una visibilidad completa y capacidad de respuesta en diversas capas de seguridad, como los dispositivos finales, la red y la nube. Estas plataformas utilizan inteligencia artificial para correlacionar datos y automatizar respuestas ante amenazas.
- SIEM (Gestión de Información y Eventos de Seguridad): Herramienta que recopila, analiza y relaciona eventos de seguridad usando machine learning para detectar amenazas avanzadas.
- EDR (Detección y Respuesta en Puntos Finales): Se centra en monitorear y responder a comportamientos sospechosos en dispositivos finales, usando IA para detectar anomalías y actuar en tiempo real.
- Firewalls de próxima generación (NGFW): Permiten controlan el tráfico de red usando reglas inteligentes y IA para bloquear ataques sofisticados.
- Los sistemas IDS (Detección de Intrusiones): Vigilan la red en busca de actividades sospechosas, mejorando la precisión y reduciendo falsas alarmas con ayuda de la IA.
- Las herramientas de escaneo de vulnerabilidades: Identifican fallas en sistemas y priorizan riesgos para recomendar soluciones.
- SOAR (Security Orchestration, Automation and Response): Es una plataforma que ayuda a las organizaciones a coordinar y automatizar la respuesta a incidentes de ciberseguridad.

La siguiente imagen se presentan las herramientas de ciberseguridad más utilizadas en las empresas para la inteligencia de amenazas y la defensa cibernética, organizadas según su tipo y frecuencia de uso. Este panorama refleja las soluciones tecnológicas que hoy se consideran esenciales para proteger la información y responder eficazmente a los crecientes riesgos digitales.

Imagen 2: Herramientas de ciberseguridad con más frecuencia de uso



La tabla refleja cómo cada vez más empresas están tomando en serio la seguridad digital y adoptando medidas para protegerse contra las amenazas cibernéticas. Gracias a la integración de la inteligencia artificial, muchas de estas herramientas pueden procesar grandes volúmenes de datos con rapidez, reducir las falsas alarmas, automatizar las respuestas y enfrentar ataques cada vez más sofisticados, incluyendo aquellos que emplean IA generativa tanto para defenderse como para atacar. Este ritmo acelerado de adopción confirma que la IA se ha convertido en una pieza fundamental para la seguridad en el mundo digital actual.

5. Resultados y Discusión

Ante lo expuesto en el documento, se puede indicar que la inteligencia artificial (IA) se presenta como una herramienta fundamental en nuestra actualidad y más aún en el ámbito de la inteligencia de amenazas y la defensa cibernética. La IA permite realizar pronósticos predictivos basados en la información acumulada y el aprendizaje continuo, lo que facilita anticipar posibles amenazas en el menor tiempo posible. Sin embargo, esta misma capacidad de automatización y sofisticación también está siendo aprovechada por los atacantes para ejecutar ciberataques más complejos y avanzados, lo que genera una preocupación creciente en el campo de la ciberseguridad.

La IA ha revolucionado las herramientas de ciberseguridad ya que ha potenciado su escala de detección, esto lo podemos encontrar por ejemplo en XDR y SIEM, que aplican algoritmos avanzados para identificar comportamientos sospechosos, incluso ataques de día cero que suelen ser difíciles de detectar.

Además, la IA facilita la integración y coordinación de diversas herramientas de seguridad, unificando flujos de trabajo y liberando al equipo humano para concentrarse en tareas estratégicas. Esto aumenta la productividad de los equipos de operaciones de seguridad (SecOps) al priorizar y contextualizar las alertas. No obstante, se reconoce que la participación humana sigue siendo clave, ya que el juicio crítico y la interpretación contextual son imprescindibles para tomar decisiones complejas.

Entre las limitaciones actuales destacan la calidad variable de los datos, la persistencia de falsas alarmas y omisiones, vulnerabilidades frente a ataques diseñados para engañar a la IA, y la dependencia tecnológica. Para enfrentar estos desafíos, se proponen medidas como auditorías periódicas de los modelos, desarrollo de IA explicable, protección de la privacidad y mantener un equilibrio adecuado entre automatización y supervisión humana.

Por último, es clave contar con regulaciones claras y marcos éticos sólidos que aseguren un uso responsable de la inteligencia artificial. También es fundamental realizar auditorías periódicas a los modelos para detectar posibles errores o sesgos, desarrollar sistemas de IA que sean transparentes y fáciles de entender, proteger la privacidad de los datos manejados y encontrar un equilibrio adecuado entre la automatización y la supervisión humana. Esto garantiza que la tecnología se use de manera segura, justa y bajo control constante.

6. Conclusiones

La investigación sobre el papel de la inteligencia artificial (IA) en la detección de amenazas y la defensa cibernética, se destaca que la IA en la actualidad se ha vuelto fundamental para proteger nuestra información digital, ya que puede analizar grandes cantidades de datos en tiempo real, detectar patrones complejos de comportamiento malicioso y automatizar respuestas para contener incidentes rápidamente y con eficacia.

A su vez, la IA ayuda a aliviar la carga de trabajo de los equipos de seguridad al reducir considerablemente las falsas alarmas, priorizar las alertas importantes y optimizar el uso de recursos humanos y técnicos. Sin embargo, es esencial mantener un equilibrio donde la automatización sea complementada por el juicio y la experiencia de los analistas humanos, quienes interpretan contextos complejos y toman decisiones estratégicas.

El futuro de la ciberseguridad estará profundamente marcado por la evolución de la inteligencia artificial. Su adopción debe ser responsable, combinando innovación tecnológica con principios éticos y cooperación entre el sector público y privado para fortalecer la capacidad de defensa global ante amenazas digitales cada vez más sofisticadas.

Referencias

[1]. Verizon. (2023). 2023 Data Breach Investigations Report. Verizon. https://www.verizon.com/about/news/2023-data-breach-investigations-report

[2]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://ieeexplore.ieee.org/document/7307098

[3]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy. https://ieeexplore.ieee.org/document/5504793

[4]. IBM. (s.f.). Threat Intelligence: Qué es y cómo usarla. IBM. https://www.ibm.com/mx-es/topics/threat-intelligence

[5]. IBM. (s.f.). Inteligencia de amenazas: Qué es y cómo usarla. IBM. https://www.ibm.com/es-es/topics/threat-intelligence

[6]. Check Point. (s.f.). ¿Qué es la inteligencia de amenazas? Check Point. https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-threat-intelligence/

[7]. OpenText. (s.f.). ¿Qué es la inteligencia de amenazas? OpenText. https://www.opentext.com/es-es/que-es/threat-intelligence

[8]. Geekflare. (s.f.). Plataformas de ciberseguridad potenciadas por IA. https://geekflare.com/es/ai-powered-cybersecurity-platforms/

[9]. Noralma Nathaly, A. (2024). Impacto de la inteligencia artificial en la ciberseguridad (Trabajo de titulación). Universidad Técnica de Babahoyo. https://dspace.utb.edu.ec/bitstream/handle/49000/15738/PI-UTB-FAFI-SIST-00011.pdf?sequence=1&isAllowed=y

[10]. Centeno Córdova, J.; Farias Estacio, A. (2024). Modelos de inteligencia artificial para prevención de ataques cibernéticos en organizaciones (Tesis de maestría). Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/27884/1/UPS-GT005371.pdf

[11]. Martín Martín, M. (2023). Inteligencia artificial: Un estudio de su impacto en ciberseguridad (Trabajo de fin de grado). Universitat Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/150519/6/mmartinmartin4TFG0624memoria.pdf

[12]. Wikipedia. (2024). Inteligencia artificial. Recuperado de https://es.wikipedia.org/wiki/Inteligencia_artificial

[13]. Russell, S., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach. Prentice Hall.

[14]. Boden, M.A. (2017). Artificial Intelligence: A Very Short Introduction. Oxford University Press.

[15]. Foro Consultivo Científico y Tecnológico. (n.d.). Inteligencia artificial. Recuperado de https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf

[16]. Logicalis. (2023). ¿Cómo afecta la IA en la propagación de los ataques cibernéticos? Recuperado de https://www.la.logicalis.com/es/Como-afecta-la-IA-en-la-propagacion-de-los-ataques-ciberneticos

[17]. Pirani Risk. (2023). Inteligencia artificial para hacer frente a los ataques cibernéticos. Recuperado de https://www.piranirisk.com/es/blog/inteligencia-artificial-ia-contra-ataques-ciberneticos
[18]. Malwarebytes. (2023). Riesgos de IA y Ciberseguridad | Riesgos de la Inteligencia Artificial. Recuperado de https://www.malwarebytes.com/es/cybersecurity/basics/risks-of-ai-in-cyber-security
[19]. PMG SSI. (2015). ISO 27001: Amenazas y vulnerabilidades. Recuperado de https://www.pmg-ssi.com/2015/04/iso-27001-amenazas-y-vulnerabilidades/
[20]. Escuela Europea Excelencia. (2019). Listado de amenazas y vulnerabilidades en ISO 27001. Recuperado de https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/
[21]. OpenKM. (2024). ISO 27000. Recuperado de https://www.openkm.com/es/blog/iso-27000.html
[22]. ISO27000.es. (n.d.). Glosario - ISO27000. Recuperado de https://www.iso27000.es/glosario.html
[23]. ISO27000.es. (n.d.). Anexo 12 - ISO 27001. Recuperado de https://www.iso27000.es/iso27002_12.html
[24]. Kaspersky. (2019). ¿Qué es la inteligencia de amenazas? Definición y explicación. Recuperado de https://latam.kaspersky.com/resource-center/definitions/threat-intelligence
[25]. IBM. (2022). ¿Qué es la inteligencia de amenazas? Recuperado de https://www.ibm.com/es-es/topics/threat-intelligence
[26]. Zscaler. (2024). ¿Qué es la inteligencia sobre amenazas? Recuperado de https://www.zscaler.com/es/zpedia/what-is-threat-intelligence
[27]. Cloudflare. (2025). ¿Qué es la información sobre amenazas? Recuperado de https://www.cloudflare.com/es-es/learning/security/glossary/what-is-threat-intelligence/
[28]. Elastic. (2025). Guía integral de inteligencia de amenazas. Recuperado de https://www.elastic.co/es/what-is/threat-intelligence
[29]. Kaspersky. (2024). ¿Qué es la ciberseguridad? Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
[30]. AWS. (2024). ¿Qué es la ciberseguridad? Recuperado de https://aws.amazon.com/es/what-is/cybersecurity/
[31]. Club CISO. (2024). Conceptos clave de ciberseguridad. Recuperado de https://club-ciso.aec.es/conceptos-clave-de-ciberseguridad/
[32]. Fortinet. (2024). ¿Qué es Ciberseguridad? Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity
[33]. IBM. (2024). ¿Qué es la ciberseguridad? Recuperado de https://www.ibm.com/es-es/topics/cybersecurity
[34]. Splashtop. (2025, junio 13). Las 12 principales tendencias y predicciones de ciberseguridad. Recuperado de https://www.splashtop.com/es/blog/cybersecurity-trends-2025
[35]. NeverOff Technology. (2025, enero 1). Ciberseguridad 2025: Nuevas amenazas para las tecnologías. Recuperado de https://neverofftechnology.com/blog/ciberseguridad-2025-nuevas-amenazas-para-las-tecnologias
[36]. WeLiveSecurity. (2025, enero 24). Ciberseguridad e inteligencia artificial: ¿qué nos depara 2025? Recuperado de

https://www.welivesecurity.com/es/seguridad-digital/ciberseguridad-ai-inteligencia-artificial-ia-2025/
[37]. Bittnet. (2025, mayo 21). Inteligencia Artificial: la principal amenaza cibernética en 2025. Recuperado de https://www.bittnet.ro/es/noutati/inteligenta-artificiala-devine-principala-amenintare-cibernetica-in-2025
[38]. Cesuma. (2025). Ciberseguridad impulsada por Inteligencia Artificial. Recuperado de https://www.cesuma.mx/blog/ciberseguridad-impulsada-por-inteligencia-artificial.html
[39]. AITEC. (2025). CrowdStrike revoluciona la ciberseguridad con Charlotte AI. AITEC. https://www.aitec.com/crowdstrike-charlotte-ai
[40]. CrowdStrike. (2025). Global threat report para el 2025. CrowdStrike. https://www.crowdstrike.com/global-threat-report-2025
[41]. Certiprof. (2025). Las 10 mejores herramientas de ciberseguridad para 2025. Certiprof. https://certiprof.com/blog/las-10-mejores-herramientas-de-ciberseguridad-para-2025
[42]. Fortinet. (2025). Fortinet impulsa la ciberseguridad de mano de la IA y sus partners. Fortinet. https://www.fortinet.com/es/partners/fortinet-impulsa-ciberseguridad-ia
[43]. TIVIT & IBM. (2025). TIVIT y IBM lanzan solución inteligente de ciberseguridad para empresas. TIVIT. https://www.tivit.com/noticias/tivit-ibm-solucion-inteligente-ciberseguridad
[44]. Unite.AI. (2025). Las 10 mejores herramientas de ciberseguridad con IA. Unite.AI. https://www.unite.ai/es/ai-cybersecurity-tools
[45]. Vectra AI. (2025). Vectra AI, la solución de seguridad potenciada con IA. Vectra AI. https://www.vectra.ai/es/soluciones
[46]. Vectra AI. (2025). Inteligencia Artificial aplicada a la ciberseguridad. Vectra AI. https://www.vectra.ai/es/inteligencia-artificial
[47]. IT Ahora. (2025). El poder de la IA en la plataforma líder de ciberseguridad Check Point Infinity AI. IT Ahora. https://www.itahora.com/noticias/check-point-infinity-ai
[48]. Splunk. (2025). Splunk revela la necesidad crítica de operaciones de seguridad impulsadas por IA. Splunk. https://www.splunk.com/es/news/splunk-operaciones-seguridad-ia
[49]. SergioJMazure. (2025, febrero 9). IA y Ciberseguridad: El Escudo Digital del 2025. Recuperado de https://sergio.ec/ia-y-ciberseguridad-el-escudo-digital-del-2025/
[50]. Digital Robots. (2025, marzo 6). El Impacto de la Inteligencia Artificial en la Ciberseguridad para 2025. Recuperado de https://www.digital-robots.com/noticias/el-impacto-de-la-inteligencia-artificial-en-la-ciberseguridad-para-2025
[51]. Licencias OnLine. (2025, febrero 11). Zero Trust e IA, un dúo que revolucionará la ciberseguridad en 2025. Recuperado de https://www.licenciasonline.com/ec/es/noticias/zero-trust-e-ia-un-d%C3%BAo-que-revolucionar%C3%A1-la-ciberseguridad-en-2025
[52]. WeLiveSecurity. (2025, enero 24). Ciberseguridad e inteligencia artificial: ¿qué nos depara 2025? Recuperado de https://www.welivesecurity.com/es/seguridad-digital/ciberseguridad-ai-inteligencia-artificial-ia-2025/
[53]. Reto. (2025, enero 14). ¿Cómo la Inteligencia Artificial Está Transformando la Ciberseguridad en 2025? Recuperado de

https://reto.com.mx/como-la-inteligencia-artificial-esta-transformando-la-ciberseguridad-en-2025/

[54]. Dreamlab. (2025, marzo 28). La revolución de la inteligencia artificial en la ciberseguridad 2025. Recuperado de https://dreamlab.net/es/blog/la-revolucion-de-la-inteligencia-artificial-en-la-ciberseguridad-2025/

[55]. ThinkersPro. (2024). Ética en la Inteligencia Artificial: Desafíos y Soluciones Clave. Recuperado de https://thinkerspro.com/etica-en-la-inteligencia-artificial-desafios-y-soluciones/

[56]. UNESCO. Ética de la inteligencia artificial. Recuperado de https://www.unesco.org/es/artificial-intelligence/recommendation-ethics

[57]. UNIR. (2025). La IA aplicada a la Ciberseguridad: Ventajas y desafíos. Recuperado de https://ecuador.unir.net/actualidad-unir/ia-ciberseguridad-ventajas-desafios/

[58]. El Comercio. (2024). La ética digital, ciberseguridad e inteligencia artificial. Recuperado de https://www.elcomercio.com/opinion/editorial/etica-digital-ciberseguridad-lorena-naranjo-columnista/

[59]. Metacompliance. (2025). AI Cyber Security: Ventajas y desafíos de la IA en ciberseguridad. Recuperado de https://www.metacompliance.com/es/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security/

[60]. Mobiledatas. (2025). Desafíos éticos en tiempos de IA: ¿Quién controla al algoritmo? Recuperado de https://mobiledatas.com/2025/05/02/desafios-eticos-en-tiempos-de-ia-quien-controla-al-algoritmo/