
# UNIVERSIDAD POLITÉCNICA SALESIANA

## SEDE QUITO

### CARRERA DE COMPUTACIÓN

# ESTADO DEL ARTE DE T ´ECNICAS DE INTELIGENCIA ARTIFICIAL QUE APORTEN EN LA CIBERSEGURIDAD

**Trabajo de titulación previo a la obtención del Título de Ingeniera en Ciencias de la Computación**

**AUTORA: ARACELLY FERNANDA ALVAREZ CUEVA**

**TUTOR: JOSE LUIS AGUAYO MORALES**

Quito - Ecuador
2024

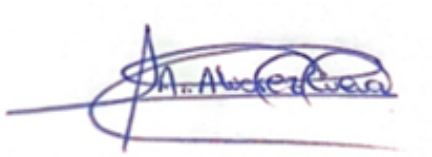
# CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Aracelly Fernanda Alvarez Cueva con documento de identificación N° 1752770121 manifiesto que:

Soy la autora y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total, o parcial el presente trabajo de titulación.

Quito, 05 de marzo del 2024

Atentamente,



Aracelly Fernanda Alvarez Cueva
1752770121

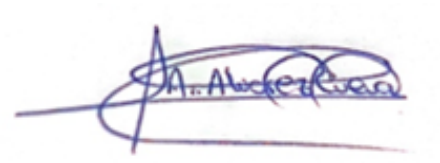
# CERTIFICADO DE CESIÓN DE DERECHOS DE AUTORA DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Aracelly Fernanda Alvarez Cueva con documento de identificación No. 1752770121, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autora del Artículo Académico: "Estado del arte de técnicas de inteligencia artificial que aporten en la ciberseguridad", el cual ha sido desarrollado para optar por el título de: Ingeniera en Ciencias de la Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 05 de marzo del 2024

Atentamente,



Aracelly Fernanda Alvarez Cueva
1752770121

# CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Ing. Jose Luis Aguayo Morales con documento de identificación N° 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ESTADO DEL ARTE DE TECNICAS DE INTELIGENCIA ARTIFICIAL QUE APORTEN EN LA CIBERSEGURIDAD, realizado por Aracelly Fernanda Alvarez Cueva con documento de identificación N° 1752770121, obteniendo como resultado final el trabajo de titulación bajo la opción de Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 05 de marzo del 2024

Atentamente,

Ing. José Luis Aguayo Morales, MSc
1729562597

# DEDICATORIA

Llena de regocijo, de amor y esperanza, dedico este artículo, a las siguientes personas:

A mi madre Rosa Cueva, porque ella ha sido el pilar y motivación de mi vida y mi orgullo, con su bendición me ha guiado a ser la persona que seré.

A mi hermana Joselyn, porque ha sido la persona que me ha acompañado en los momentos más difíciles de esta carrera y por siempre confiar en mí y que lo lograría.

Y sin dejarlos atrás a mis amigos por los buenos momentos que compartí con ustedes en la universidad, aprender de cada uno de ustedes y por siempre estar presentes.

# ESTADO DEL ARTE DE TÉCNICAS DE INTELIGENCIA ARTIFICIAL QUE APORTEN EN LA CIBERSEGURIDAD
# STATE OF THE ART OF ARTIFICIAL INTELLIGENCE TECHNIQUES CONTRIBUTING TO CYBERSECURITY

1st Aracelly Fernanda Alvarez Cueva
aalvarezc3@est.ups.edu.ec

2nd Jose Luis Aguayo Morales
jaguayo@ups.edu.ec

***Resumen*—La investigación actual examina las técnicas de inteligencia artificial IA que aportan en ciberseguridad mediante mapeo y revisión sistemática de la literatura durante el período comprendido entre 2018 y 2023. Se utilizó el método PICOC y se formularon preguntas relacionadas con la investigación. Se aplicaron requisitos para la selección y exclusión en tres etapas de filtrado, resultando en la selección de 30 estudios. La taxonomía identificó diversas técnicas de IA, como XAI, BT-AI, aprendizaje automático, aprendizaje incremental, machine learning y aprendizaje profundo. Se concluyó que estas técnicas aportan un papel clave en fortalecer la ciberseguridad, abordando amenazas como ataques DoS, Malware y Ransomware. Se examinaron herramientas relacionadas con la IA, como Big Data, IoT, UML, análisis experimental, reglas de asociación y análisis factorial confirmatorio, resaltando su contribución en la protección contra ataques cibernéticos. Se abordó la variedad de riesgos, desde ataques DoS hasta protección para los sistemas de gestión de bases de datos, subrayando una necesidad constante de estrategias innovadoras para proteger sistemas y datos en el ciberespacio.**

***Palabras Clave*—seguridad de la información, inteligencia artificial, gestión, evaluación de seguridad, aprendizaje automático, ciberseguridad.**

***Abstract*—The current research examines artificial intelligence (AI) techniques contributing to cybersecurity through mapping and a systematic literature review covering the period from 2018 to 2023. The PICOC method was employed, and research-related questions were formulated. Requirements for selection and exclusion were applied in three filtering stages, resulting in the selection of 30 studies. The taxonomy identified various AI techniques, such as Explainable AI (XAI), BT-AI, machine learning, incremental learning, and deep learning. It was concluded that these techniques play a key role in strengthening cybersecurity, addressing threats such as Denial-of-Service (DoS) attacks, malware, and ransomware. Tools related to AI were examined, including Big Data, IoT, UML, experimental analysis, association rules, and confirmatory factor analysis, highlighting their contribution to protecting against cyber attacks. A variety of risks were addressed, from DoS attacks to protection for database management systems, emphasizing a constant need for innovative strategies to safeguard systems and data in cyberspace.**

***Keywords*—information security, artificial intelligence, manage, security evaluation, machine learning, and cyber security.**

## I. Introducción

El mapeo sistemático es una técnica de investigación que busca recopilar, evaluar y sintetizar de manera sistemática la evidencia disponible sobre un tema específico. Su objetivo claro incluye identificar brechas en la investigación, evaluar la calidad de la evidencia o elaborar recomendaciones. Se sigue una metodología estructurada con criterios de inclusión y exclusión, búsqueda exhaustiva y métodos transparentes. La síntesis de resultados revela patrones y tendencias, a menudo presentados visualmente. Se realiza una evaluación crítica de la calidad de los estudios incluidos, contribuyendo a la validez de las conclusiones. La transparencia en la metodología y la documentación permite la reproducibilidad.

La revisión de lectura sistemática es un proceso metódico y estructurado para analizar y sintetizar la literatura existente sobre un tema específico. En este tipo de revisión, se establecen criterios claros para la selección de estudios, se realiza una búsqueda exhaustiva de la literatura y se aplica una metodología sistemática para evaluar la calidad de los estudios incluidos. Los resultados se sintetizan de manera rigurosa para identificar patrones, tendencias y brechas en la investigación. La revisión de lectura sistemática contribuye a una comprensión más profunda del estado actual del conocimiento sobre un tema y puede proporcionar una base sólida para la toma de decisiones, la identificación de áreas de investigación futura y la formulación de recomendaciones. La transparencia en el proceso y la documentación detallada son fundamentales para garantizar la reproducibilidad y la confiabilidad de los resultados de la revisión de lectura sistemática. La ciberseguridad ha surgido como un desafío crítico en la era digital, donde la globalización y la dependencia en la tecnología ha aumentado exponencialmente. En este contexto,las técnicas basadas

en la IA se han convertido en fundamentales para fortalecer las defensas contra las amenazas cibernéticas. El ”Estado del arte de técnicas de Inteligencia Artificial en ciberseguridad” representa un campo de estudio en constante evolución que busca abordar las vulnerabilidades y riesgos asociados con las infraestructuras digitales. En los últimos años, la comunidad investigativa y de desarrollo para el ámbito de la seguridad cibernética ha experimentado avances significativos, impulsados por la capacidad transformadora de la IA. Una de las áreas destacadas es utilizando algoritmos de aprendizaje automático para detectar amenazas. Estos algoritmos pueden examinar patrones de comportamiento, anomalías en grandes conjuntos de datos, permitiendo una identificación temprana de actividades maliciosas. Desde el aprendizaje supervisado hasta las técnicas más avanzadas de aprendizaje profundo, la capacidad de la IA para adaptarse y aprender de nuevas amenazas la convierte en una herramienta esencial para luchar contra el cibercrimen. Otro componente clave en el estado actual de la ciberseguridad es utilizando métodos de procesamiento de lenguaje natural (PLN) para una identificación de ataques de ingeniería social, mejora de la detección de malware. La comprensión contextual y semántica del lenguaje permite a los sistemas de IA discernir mensajes engañosos o enlaces maliciosos, brindando una capa adicional de protección contra tácticas de manipulación humana. Además, la orquestación y automatización de respuestas a incidentes cibernéticos son áreas en las que la IA ha demostrado su eficacia. Los sistemas de respuesta automática basados en reglas y algoritmos de toma de decisiones pueden reducir los tiempos de respuesta frente a amenazas, minimizando el impacto de posibles ataques. Este estado del arte no solo destacan los logros actuales, sino también las áreas de investigación emergentes que prometen impulsar aún más la incorporación de la IA en la ciberseguridad. Desde una mejora de la resiliencia contra ataques adversarios hasta la anticipación de riesgos futuros, la combinación de la IA y la ciberseguridad se presenta como un terreno fértil para la innovación y la defensa digital [1]. Para tener una mejor visión de cómo ha sido el aporte de la inteligencia artificial a la cibersegruidad en estos últimos cinco años; se ha realizado un MS-IA-CG (Systematic Mapping of Artificial Intelligence in cybersecurity) y una LS-IA-CG de (Systematic reading of Artificial Intelligence in Cybersecurity).

## II. Métodología

La investigación que se presenta a continuación empleó la metodología de MS-IA-CG (mapeo sistématico). El MS-IA-CG se centra en identificar, reconocer y categorizar las técnicas de IA en ciberseguridad, mientras que el LS-IA-CG (lectura sistemática) facilita la planificación, ejecución y documentación de la revisión sistemática. El objetivo consiste en adquirir una referencia más exacta acerca de las investigaciones llevadas a cabo entre los años 2018 y 2023. Se describen a las técnicas de Inteligencia Artificial como la fusión de algoritmos propuestos con el propósito de crear máquinas que demuestren habilidades equiparables a las de los seres humanos.

Con el propósito de guiar la metodología en este análisis del estado actual, se emplearon MS-IA-CG y LS-IA-CG, por lo cual se organizó de la siguiente manera: Para la primera etapa, establecemos objetivos y la extensión de los parámetros de elección. Para la segunda etapa, llevamos a cabo el análisis, identificando los elementos fundamentales de la investigación y dividiéndolos en dos pasos. Para la etapa final, exponemos el análisis, clasificando los estudios en distintas agrupaciones, con el objetivo de cumplir con las pautas establecidas por MS-IA-CG y LS-IA-CG.

### *A. Primera Etapa*

Para obtener árticulos vinculados a los diversos métodos de inteligencia artificial en ciberseguridad, se empleó el enfoque PICOC, el cual empleamos para exponer los elementos de búsqueda tal como se especifican en la Tabla I.

TABLA I
DESARROLLO MÉTODO PICOC

| | |
|---|---|
| Population (P): ¿Quién? | Inteligencia artificial en ciberseguridad. |
| Intervention (I): ¿Qué?, ¿Cómo? | Técnicas de inteligencia artificial. |
| Comparison (C): ¿Con qué comparar? | Estudios que presenten técnicas de inteligencia artificial en ciberseguridad. |
| Outcomes (O): ¿Qué se busca con seguir/mejorar? | Ventajas, limitaciones en las técnicas de la inteligencia artificial. |
| Context (C): ¿En qué tipo de organización y bajo qué circunstancias? | Investigar y revisar estudios sobre las técnicas de la inteligencia artificial. |

Los términos utilizados para crear la cadena de búsqueda se definen utilizando expresiones booleanas como ”AND” u ”OR” para configurar nuestra secuencia de búsqueda, como se muestra en la Tabla II: (”Ciberseguridad OR seguridad de la información” OR ”evaluación de seguridad” OR ”seguridad cibernética”) AND (”Inteligencia Artificial” OR ”aprendizaje automático”).

TABLA II
TÉRMINOS PARA REALIZAR CADENA DE BÚSQUEDA

| TÉRMINOS | TÉRMINOS SEMEJANTES |
|---|---|
| Cybersecurity | information security, security evaluación, cybersecurity |
| Artificial intelligence | artificial intelligence, machine learning |

Para seleccionar los estudios pertinentes, se aplicarán los criterios de inclusión y exclusión para MS-IA-CG y

LS-IA-CG.

Los criterios para excluir: Incluían textos que no estuvieran escritas en ingles, tuvieran menos de 5 páginas y fueran duplicados en revistas o conferencias, así como aquellos relacionados con técnicas de la IA que no aporten a la ciberseguridad.

Criterios de inclusión: Durante la búsqueda en un repositorio, considerando ciertos criterios, se buscó la inclusión de los términos de búsqueda empleados en los resúmenes y títulos de los artículos, según lo detallado en la Tabla 2. Llevaron a cabo búsquedas de estudios e investigaciones. Basadas en evidencia empírica que utilizaran herramientas relacionadas con técnicas de inteligencia artificial en ciberseguridad.

### *B. Segunda Etapa*

La meta principal de esta investigación es actualizar la información actual de los métodos de inteligencia artificial en la industria de la ciberseguridad. Por esta razón, se formularon las siguientes preguntas de investigación para el MS-IA-CG y LS-IA-CG:

MS-IA-CG1:¿Cuál es el estado actual de los diferentes sectores que usan IA para mejorar su ciberseguridad?

MS-IA-CG2:¿Cuáles son los casos de estudio que demuestran que la IA es efectiva en la ciberseguridad?

LS-IA-CG3:¿Cuál es el objetivo principal de la revisión sistemática sobre las técnicas de la IA en la cibereguridad?

LS-IA-CG4:¿Por qué es crucial implementar IA en el ámbito de la ciberseguridad?

En la estrategia de búsqueda: Se implementó una recopilación en un repositorio, como se puede observar la Tabla III, el cual fue seleccionado previamente para asegurar la disponibilidad de artículos que respalden un estudio de Mapeo Sistemático MS-IA-CG y Revisión de la Literatura Sistemática LS-IA-CG. Para la primera fase de filtrado, se recolectaron 4429 estudios primarios. En el repositorio IEEE, se estableció el rango de búsqueda entre 2018 y 2023, optimizando el patrón para realizar la búsqueda.

La cadena de búsqueda se utiliza en los títulos y resúmenes durante la segunda fase de filtrado con el software EndNote x9. Como resultado, la cantidad de estudios ha disminuido considerablemente a 192.

La tercera etapa de filtrado, se bajaron los textos completos y se realizaron lecturas individuales de cada texto. Durante este proceso, se seleccionaron 30 estudios utilizando criterios de inclusión y exclusión.

TABLA III
CADENA DE BÚSQUEDA PARA EL REPOSITORIO

| REPOSITORIO | CADENA DE BÚSQUEDA | TIPO DE ARTÍCULO | FILTRO 1 | FILTRO 2 | FILTRO 3 |
|---|---|---|---|---|---|
| IEEE | Title: "artificial intelligence" OR "cybersecurity management" OR "information security" OR "security evaluation" | Revistas, conferencias | 4429 | 192 | 30 |

### *C. Tercera Etapa*

Para la obtención de los diferentes tipos de técnicas de IA en ciberseguridad en la actualidad, se extrajo la información de los artículos identificados en las etapas anteriores, se busca responder preguntas de investigación para MS-IA-CG y LS-IA-CG. Después de recopilar información de estudios, lo siguiente a realizar es una síntesis de información, que se llega a recapitular en una taxonomía, como se ilustra en la Figura 1, lo que facilita la comparación de la recopilación de datos. Esto brindará conciencia necesaria para abordar las preguntas relacionadas con el estado actual del conocimiento.

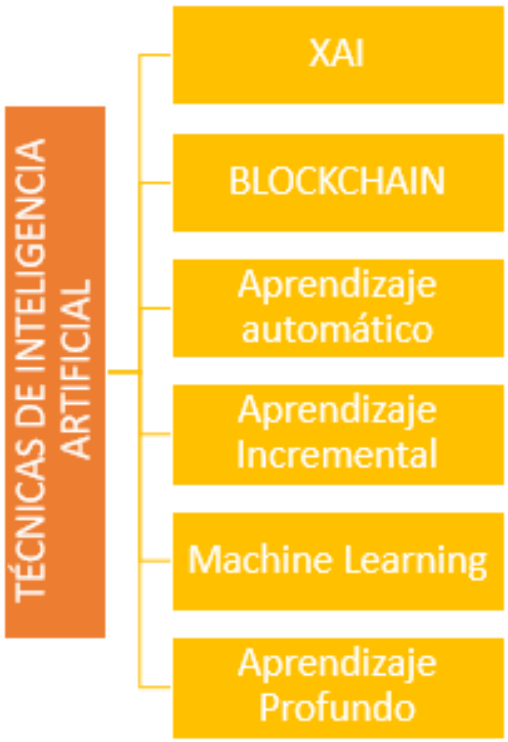



Fig. 1: Taxonomia de las técnicas de la (IA) en ciberseguridad

Cada uno de estos se detallaran a continuación:

La técnica de XAI ayuda a comprender e interpretar las predicciones de los algoritmos de IA, permitiendo más claridad en el proceso automatizado de toma de decisiones de seguridad cibernética. Tambien se utiliza para introducir

explicabilidad y transparencia en las decisiones de modelos de IA, incluyendo Aprendizaje Profundo (DL) y Aprendizaje Automático (ML). En el contexto de la seguridad cibernética, la explicabilidad es esencial para defenderse de amenazas y comprender las decisiones de seguridad [2] [3].

La técnica Blockchain con Inteligencia Artificial ayuda a mejorar la seguridad y la privacidad en entornos inteligentes. La IA se emplea para abordar desafíos de seguridad, como ataques DoS, Eclipse y Doble gasto, mediante la detección y mitigación de anomalías [4].

La técnica de aprendizaje automático utilizando un SIEM proporciona un enfoque sólido para detectar riesgos cibernéticos, mejorando la eficiencia y precisión en comparación con otras técnicas como el plan de respuesta ante incidentes, el análisis de tráfico de red y el análisis de comportamiento de usuarios, entidades (UEBA) y en el (SOC) [5].

La técnica del aprendizaje incremental sirve para aplicar a algoritmos escalables que permiten el aprendizaje secuencial y la actualización continua de modelos a partir de flujos infinitos de datos. dentro de este también se encuentra el modelo de clasificación incremental donde se lo utiliza para adoptar el aprendizaje dinámico para adaptarse a entradas de datos cambiantes y enormes conjuntos de datos, destacando el algoritmo ARFC [6].

La técnica de Machine Learning (ML) es aplicada para analizar datos de sensores en sistemas de transporte y abordar desafíos relacionados con el análisis de flujo y el aprendizaje automático. Dentro de esta técnica encontramos algunos algoritmos de análisis/aprendizaje de flujo utilizados para comprender la naturaleza de los datos de transporte, especialmente aquellos que surgen como flujos de datos [7].

El aprendizaje profundo (DL) busca mejorar la eficiencia informática, abordar nuevas preocupaciones de seguridad y proteger la discreción de sensores multimedia inalámbricos mediante la implementación del aprendizaje de funciones ciegas (BFL) y la autenticación de capa física ligera (LPLA) [8].

Estas técnicas de inteligencia artificial desempeñan un papel fundamental en fortalecer la ciberseguridad. XAI garantiza la transparencia y comprensión de las decisiones de la IA, mientras que BT-AI se enfoca en el análisis del comportamiento para detectar patrones maliciosos en la red. Aprendizaje Automático y Aprendizaje Incremental permiten adaptarse y evolucionar frente a nuevas amenazas, siendo especialmente valiosos para la detección dinámica. Machine Learning analiza grandes conjuntos de datos para identificar comportamientos maliciosos, y el Aprendizaje Profundo utiliza redes neuronales para obtener representaciones complejas, mejorando la precisión en la detección de amenazas en ciberseguridad. En conjunto, estas técnicas ofrecen una defensa robusta y adaptable contra las amenazas digitales.

A continuación en la figura 2 se visualizan las herramientas que utilizan la IA en la seguridad cibernética.

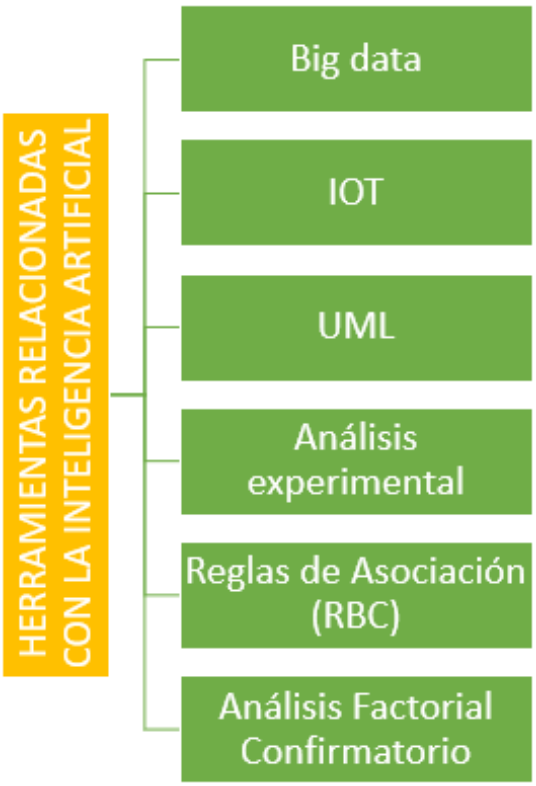



Fig. 2: Herramientas relacionadas con la IA

Estas herramientas relacionadas con la inteligencia artificial en ciberseguridad desempeñan roles cruciales en el panorama actual:

Big Data: La herramienta Big Data permite gestionar y analizar los datos. Facilitar el reconocimiento de tendencias y patrones en ciberseguridad, mejorar la detección de amenazas y proporcionar una visión holística de las actividades maliciosas en tiempo real.

IoT (Internet of Things): IoT se enfoca en asegurar los dispositivos interconectados. En ciberseguridad, esta herramienta aborda los desafíos asociados con la seguridad de la red y los dispositivos, garantizando la protección contra posibles vulnerabilidades y ataques dirigidos a la infraestructura IoT.

UML (Unified Modeling Language): UML proporciona un lenguaje estandarizado para visualizar, modelar y documentar sistemas de software. En ciberseguridad, facilita la comprensión y diseño de arquitecturas seguras, permitiendo una planificación efectiva y la identificación proactiva de

posibles debilidades.

Análisis Experimental: El análisis experimental en ciberseguridad implica la evaluación práctica de medidas de seguridad. Esta herramienta permite probar la efectividad de las soluciones en entornos controlados, identificando debilidades y refinando estrategias para fortalecer la resiliencia contra amenazas.

Reglas de Asociación (RBC): RBC se centra en descubrir patrones de relación entre variables en conjuntos de datos. En ciberseguridad, se utiliza para identificar correlaciones entre eventos, permitiendo la detección de comportamientos anómalos y la anticipación de posibles ataques basados en patrones previos.

Análisis Factorial Confirmatorio:Esta herramienta se utiliza para validar modelos teóricos mediante la confirmación de relaciones entre variables. En ciberseguridad, el Análisis Factorial Confirmatorio ayuda a evaluar la eficacia de los modelos de seguridad propuestos, garantizando una implementación sólida y adaptativa en respuesta a las amenazas emergentes.

En ciberseguridad, un conjunto de recursos de IA, como Big Data para un análisis de gran volumen de datos eficiente, IoT para una seguridad en dispositivos interconectados, UML para la planificación y diseño de arquitecturas seguras, el Análisis Experimental para evaluar medidas de seguridad en entornos controlados, Reglas de Asociación para descubrir patrones y correlaciones, y el Análisis Factorial Confirmatorio para validar modelos teóricos, colaboran de manera integral. Estas herramientas fortalecen la habilidad de anticipación, para detectar y responder de manera proactiva en respuesta a ataques cibernéticos, asegurando una defensa robusta y adaptativa en el complejo entorno de la seguridad informática.

En la siguiente figura 3 se pueden observar las amenazas que se han logrado destacar en ataques a la ciberseguridad pero han logrado ser mitigadas con ayuda de las técnicas ya antes mencionadas de la IA las cuales se pueden revisar en la figura 1.

La ciberseguridad se enfrenta a una diversidad de amenazas cada vez más sofisticadas y persistentes. Desde el riesgo de ataques de malware, ransomware y phishing que buscan explotar vulnerabilidades en sistemas y redes, hasta amenazas más avanzadas como ataques de ingeniería social que aprovechan la manipulación psicológica. Además, el surgimiento de riesgos emergentes como la IA maliciosa y un aumento de ataques a dispositivos IoT añaden complejidad al panorama de la seguridad cibernética. En la vulnerabilidad de infraestructura importante, la proliferación de ataques a la nube y la falta de conciencia de seguridad en los usuarios representan desafíos adicionales. La rápida evolución de estas amenazas subraya la necesidad constante de estrategias y soluciones innovadoras para salvaguardar La confidencialidad, la integridad y la disponibilidad de los datos en un ciberespacio.


Fig. 3: Amenazas que enfrenta la ciberseguridad

A continuación en la figura 3 se resumen las amenazas encontradas:

Ataques DoS (Denegación de Servicio):Los ataques DoS buscan abrumar el sistema, de red o servicio saturado, incapacitando su capacidad para hacer frente a solicitudes justificadas. La IA contribuye al detectar patrones anómalos y mitigar estos ataques en tiempo real.

Eclipse: Un eclipse implica aislar un nodo o sistema al inundarlo con información falsa o controlarlo para interceptar y manipular su tráfico. La IA ayuda a identificar comportamientos sospechosos y defender contra la manipulación de nodos.

Malware: El software malicioso se conoce como malware y está diseñado para dañar o acceder no autorizadamente a un sistema. La IA fortalece la ciberseguridad al analizar comportamientos anómalos y patrones para detectar y prevenir la propagación del malware.

Scareware: Scareware busca engañar a los usuarios mediante mensajes falsos de amenazas, insitándolos a comprar software innecesario. La IA contribuye a la identificación y bloqueo proactivo de este tipo de tácticas engañosas.

Amenazas Persistentes Avanzadas (APT): Las APT son ataques prolongados y sigilosos, a menudo respaldados por actores estatales. La IA ayuda a detectar patrones de comportamiento no típicos y actividades sospechosas, mejorando la capacidad de defensa contra amenazas persistentes.

Ransomware: El ransomware cifra los datos y exige un rescate para la liberación de estos mismos. La IA contribuye a la detección temprana y respuesta rápida, así como a la prevención mediante análisis de comportamiento y patrones asociados con ransomware.

Cifrado Fuerte: El cifrado fuerte es crucial para proteger datos sensibles. La IA se aplica para mejorar algoritmos de cifrado, detectar debilidades y garantizar la confidencialidad e integridad de la información.

Violaciones de Privacidad: Hay violaciones de privacidad que involucran el acceso a datos no autorizados a información personal. La IA ayuda a identificar y prevenir estas violaciones mediante el análisis continuo de patrones de acceso y comportamientos inusuales.

Aislamiento de Datos: El aislamiento de datos busca proteger información sensible limitando su acceso. La IA refuerza estas medidas mediante la identificación de intentos de acceso no autorizado y detectar cualquier anomalía en la conducta del usuario.

Vulnerar Sistemas Gestores de Bases de Datos: La vulneración a sistemas para administrar bases de datos implica el acceso no autorizado a información almacenada. La IA mejora al detectar intentos de infiltración y protege contra actividades anómalas.

Detecciones Falsas: Las detecciones falsas ocurren cuando sistemas de seguridad generan alertas incorrectas. La IA contribuye a reducir falsos positivos al mejorar la precisión de los algoritmos de detección y aprendizaje automático.

## III. RESULTADOS

En la tabla IV se muestra las técnicas de la IA encontradas al momento de realizar el mapeo y la revisión de lectura sistemática mostrandonos el paorte que realiza cada una de las técnicas en el ambito de la ciberseguridada

TABLA IV: TÉCNICAS DE LA IA Y SU APORTE EN LA CIBERSEGURIDAD

| TÉCNICAS | APORTE A LA CIBERSEGURIDAD |
|---|---|
| XAI | Ayuda a mejorar la confianza, la comprensión y la eficacia de los sistemas de inteligencia artificial utilizados para prevenir, detectar y responder a amenazas cibernéticas. La capacidad de interpretar y explicar las decisiones de estos sistemas es crucial para el éxito y la aceptación de la inteligencia artificial en el ámbito de la seguridad informática. |
| BLOCKCHAIN | Contribuye a la gestión segura de identidad y acceso, mediante contratos inteligentes seguros y la capacidad de rastrear actividades de forma transparente. La descentralización de la blockchain ayuda a mitigar ataques DDoS y su transparencia fomenta la confianza en la compartición segura de información entre partes. Sin embargo, se destaca que la implementación efectiva de esta tecnología requiere consideración cuidadosa de los riesgos y la integración con otras prácticas de seguridad. |
| APRENDIZAJE AUTOMÁTICO | Mejora la detección de amenazas, permite la adaptación a nuevas tácticas de ataque y facilita respuestas más rápidas frente a incidentes. Los algoritmos de aprendizaje automático son eficaces para clasificar y prever comportamientos maliciosos, contribuyendo así a fortalecer la postura de seguridad y proteger activos digitales. Es fundamental para abordar la creciente complejidad y sofisticación de las amenazas cibernéticas al proporcionar capacidades avanzadas de análisis y respuesta. |
| APRENDIZAJE INCREMENTAL | Permite a los sistemas de seguridad aprender de forma progresiva, incorporando información en tiempo real para ajustar sus modelos y mejorar la detección y respuesta ante amenazas. La adaptabilidad constante a través del aprendizaje incremental fortalece la capacidad de los sistemas de ciberseguridad para hacer frente a tácticas de ataque en constante evolución y |

| | |
|---|---|
| | garantiza una defensa más efectiva contra las amenazas emergentes. |
| MACHINE LEARNING | Mejora la capacidad de identificación de amenazas, facilita la adaptación a nuevas tácticas de ataque y agiliza la respuesta frente a incidentes. Los algoritmos de aprendizaje automático son eficaces para clasificar comportamientos maliciosos, fortaleciendo así la postura de seguridad y protegiendo activos digitales. Su aplicación es esencial para enfrentar la complejidad creciente de las amenazas cibernéticas al ofrecer capacidades avanzadas de análisis y respuesta. |
| APRENDIZAJE PROFUNDO | Es especialmente útil para la detección de amenazas, como el reconocimiento de patrones de comportamiento malicioso o la identificación de vulnerabilidades. Su capacidad para procesar información no estructurada y adaptarse a cambios en el panorama de amenazas hace que el aprendizaje profundo sea una herramienta poderosa para fortalecer las defensas cibernéticas y mejorar la respuesta a incidentes. |

A continuación se muestra un analisis realizado donde los resultados cuantitativos son el número de veces que se encontró cada una de las herramientas relacionadas a la ciberseguridad en los árticulos y de la misma manera de las técnicas de la IA.


Fig. 4: Análisis de Dataset de las herramientas realcioandas con la IA

La figura 4 nos muestra que de los 30 artículos de nuestro DATASET analizado podemos observar en la imagen que nueve hablan sobre Big Data, tres de IOT, uno sobre UML, uno sobre Análisis Experimental, dos de Reglas de Asociación, y uno de Análisis factorial confirmado estas son herramientas relacionadas con la IA y contribuyen a fortalecer las capacidades de ciberseguridad al permitir la detección temprana, la respuesta rápida y la mejora continua de las defensas contra amenazas.

En la figura 5 de igual manera nos muestra que los artículos que se encuentran en nuestro DATASET, se observa en la imagen que dos se hablan sobre XAI, dos de Blockchain, tres de Aprendizaje Automático, doce de Aprendizaje Incremental, uno de Machine Learning y ocho de aprendizaje profundo, estas técnicas abordan desafíos en comprensión,

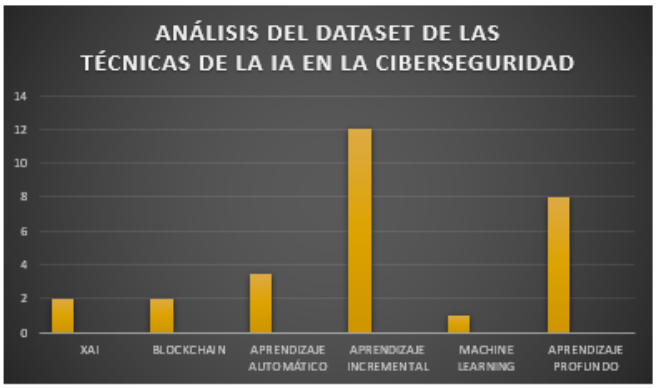



Fig. 5: Análisis de Dataset de las técnicas de la IA en la ciberseguridad

seguridad, adaptabilidad y capacidad de procesamiento, impulsando avances significativos para la ciberseguridad.

## IV. CONCLUSIÓN

Las técnicas de inteligencia artificial (IA) han emergido como un pilar fundamental en el ámbito de la ciberseguridad, ofreciendo soluciones avanzadas y adaptables para hacer frente a las crecientes y sofisticadas amenazas digitales. La capacidad de aprendizaje automático de la IA permite una detección proactiva y dinámica de patrones maliciosos, contribuyendo a la anticipación y prevención de ataques.

En la detección de amenazas, la IA ha mejorado significativamente la capacidad de identificar comportamientos anómalos y ataques específicos, incluso aquellos que evolucionan rápidamente. El Machine Learning y el Aprendizaje Profundo examina vastos conjuntos de datos en tiempo real con el fin de identificar patrones y relaciones que puedan pasar desapercibidos para las técnicas convencionales.

La interpretabilidad y transparencia de la explicabilidad en la IA, como en el caso de XAI, han llevado a un entendimiento más profundo de las decisiones automáticas, generando confianza y facilitando la colaboración entre sistemas automatizados y profesionales de la ciberseguridad.

El análisis de comportamiento, respaldado por la IA, ha fortalecido la capacidad para identificar amenazas basadas en acciones y actividades anómalas, proporcionando una defensa más robusta frente a tácticas sofisticadas, como ataques de ingeniería social y ransomware.

Asimismo, la combinación de técnicas de IA con otras herramientas, como Big Data, IoT, y análisis experimental, ha ampliado las capacidades de defensa, abordando desafíos específicos como la seguridad en dispositivos interconectados y la evaluación práctica de medidas de seguridad.

No obstante, la ciberseguridad enfrenta la continua evolución de amenazas, y la IA debe adaptarse y evolucionar

constantemente para mantenerse efectiva. Además, la ética en el uso de la IA en ciberseguridad se convierte en un factor crítico, asegurando que el poder de estas tecnologías se utilice de manera responsable, sin comprometer la privacidad y los derechos individuales.

En resumen, las técnicas de inteligencia artificial no solo han transformado la forma en que abordamos la ciberseguridad, sino que también han proporcionado un impulso sustancial en la capacidad de anticipar, identificar y reaccionar ante amenazas digitales, marcando un hito significativo en la defensa de la integridad y seguridad en el ciberespacio.

## REFERENCES


[1] D. J. E. O. Y. T. G. B. Brayan Sebastián Castellanos Rojas, Carlos Uriel Cortés Rodríguez, "Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad," 2020.

[2] H. A. y. D. E. y. Y. C. Y. y. T. F. Zhang, Zhibo y Hamadi, "Aplicaciones explicables de inteligencia artificial en seguridad cibernética: investigación de vanguardia," *Acceso IEEE*, 2022.

[3] G. y. L. V. y. S. C. Capuano, Nicola y Fenza, "Inteligencia artificial explicable en ciberseguridad: una encuesta," *Acceso IEEE*, 2022.

[4] Z. y. A. E. G. y. M. B. Fadi, Oumaima y Karim, "Una encuesta sobre tecnologías blockchain y de inteligencia artificial para mejorar la seguridad y la privacidad en entornos inteligentes," *Acceso IEEE*, 2022.

[5] "A semantic machine learning algorithm for cyber threat detection and monitoring security," in *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*.

[6] V. M. M, V. Khullar, A. A. Bhosle, M. D. Salunke, J. L. Bangare, and A. Ingavale, "Streamed incremental learning for cyber attack classification using machine learning," in *2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, 2022.

[7] B. Thuraisingham, "Cyber security and artificial intelligence for cloud-based internet of transportation systems," in *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2020.

[8] X. Qiu, Z. Du, and X. Sun, "Artificial intelligence-based security authentication: Applications in wireless multimedia networks," *IEEE Access*, 2019.