593 Digital Publisher
CEIT
ISSN 2588-0705

Tendencias de las Técnicas de la Inteligencia Artificial, en la Detección de Delitos Informáticos: Revisión Sistemática de la Literatura (SLR).

Trends in Artificial Intelligence Techniques, in the Detection of Computer Crimes: Systematic Review of the Literature (SLR).

Joseph Alberto Delgado-Indacochea[1]
Universidad Técnica de Manabí, Portoviejo - Ecuador
jdelgado8240@utm.edu.ec

Roberth Abel Alcívar-Cevallos[2]
Universidad Técnica de Manabí, Portoviejo - Ecuador
roberth.alcivar@utm.edu.ec

doi.org/10.33386/593dp.2024.1.2184

V9-N1 (ene-feb) 2024, pp 810-830 | Recibido: 10 de octubre del 2023 - Aceptado: 20 de diciembre de agosto del 2023 (2 ronda rev.)

1ORCID: https://orcid.org/xxxxx0009-0009-2343-2643

2 ORCID: https://orcid.org/0000-0001-6282-8493

Cómo citar este artículo en norma APA:

Delgado-Indacochea, J. & Alcívar-Cevallos, R., (2023). Tendencias de las Técnicas de la Inteligencia Artificial, en la Detección de Delitos Informáticos: Revisión Sistemática de la Literatura (SLR).. 593 Digital Publisher CEIT, 9(1), 810-830, https://doi.org/10.33386/593dp.2024.1.2184

RESUMEN

En este artículo, se presenta una Revisión Sistemática de la Literatura (SLR) que se centra en las aplicaciones de las técnicas de Inteligencia Artificial (IA) con el propósito de detectar delitos informáticos. La primera parte de la revisión se dedica a seleccionar las fuentes de información a emplear, mientras que en la siguiente sección se proporciona una descripción detallada de las investigaciones que han empleado estas técnicas de IA. Durante este proceso de investigación, se evidenció que la mayoría de los estudios han empleado una diversidad de algoritmos de IA, entre los más frecuentes figuran SVM, Decision Tree, Logistic Regression, Naive Bayes, KNN y Random Forest, los cuales han demostrado su eficacia en múltiples áreas de ciberseguridad, abarcando la detección de intrusiones, ataques de denegación de servicio (DoS), phishing y malware. En este contexto, se ha observado que XGBoost, Random Forest y Logistic Regression destacan por su asombroso equilibrio entre las métricas de precisión y exactitud, los hallazgos enfatizan la necesidad de adaptar la elección del algoritmo según el conjunto de datos y el contexto específico, subrayando la importancia de llevar a cabo pruebas y definiciones meticulosas. Por último, los resultados obtenidos de esta revisión proporcionan una guía esclarecedora que puede orientar decisiones, ofreciendo a los lectores una visión de las técnicas más prometedoras de las áreas que ameritan mayor atención. Como conclusión se destaca que el delito informático más recurrentemente abordado en estos estudios es el Ataque de Denegación de Servicio (DoS), seguido de problemáticas asociadas al Phishing y al Malware. En cuanto a la evolución de las técnicas de inteligencia artificial para hacer frente a los desafíos emergentes en ciberseguridad, es evidente que la Inteligencia Artificial desempeñará un papel crucial en la lucha contra los delitos informáticos. Una dirección prometedora para investigaciones futuras podría ser el desarrollo de sistemas de IA capaces de aprender y adaptarse dinámicamente a nuevas amenazas. Asimismo, se sugiere explorar vías para futuras investigaciones en este ámbito.

Palabras clave: aprendizaje automático, algoritmos de inteligencia artificial, inteligencia artificial, ciberseguridad, detección de delitos informáticos.

ABSTRACT

En this article, a Systematic Literature Review (SLR) is presented that focuses on the applications of Artificial Intelligence (AI) techniques for detecting cybercrimes. The first part of the review is dedicated to selecting the sources of information to be used, while the next section provides a detailed description of the research that has employed these AI techniques. During this research process, it was evident that the majority of the studies have used a variety of AI algorithms. Among the most frequent ones are SVM, Decision Tree, Logistic Regression, Naive Bayes, KNN, and Random Forest, which have demonstrated their effectiveness in multiple areas of cybersecurity, including intrusion detection, Denial of Service (DoS) attacks, phishing, and malware. In this context, it has been observed that XGBoost, Random Forest, and Logistic Regression stand out for their remarkable balance between precision and accuracy metrics. The findings emphasize the need to adapt the choice of algorithm according to the dataset and specific context, highlighting the importance of conducting meticulous tests and definitions. Finally, the results obtained from this review provide an enlightening guide that can guide decisions, offering readers a glimpse into the most promising techniques in areas that deserve greater attention, as well as exploration for future research. In conclusion, it is highlighted that the computer crime most frequently addressed in these studies is the Denial of Service (DoS) Attack, followed by problems associated with Phishing and Malware. Regarding the evolution of artificial intelligence techniques to address emerging challenges in cybersecurity, it is evident that Artificial Intelligence will play a crucial role in the fight against cybercrime. A promising direction for future research could be the development of AI systems capable of dynamically learning and adapting to new threats. Likewise, it is suggested to explore avenues for future research in this area.

Keywords: machine learning, artificial intelligence algorithms, artificial intelligence, cybersecurity, cybercrime detection.

Introducción

El campo de la ciberseguridad se encuentra en un estado de constante evolución debido a la rápida expansión de la tecnología y la correspondiente adaptabilidad de los ciberdelincuentes. Las técnicas de Inteligencia Artificial (IA), y en particular, los algoritmos de aprendizaje automático y aprendizaje profundo han demostrado ser poderosos aliados en la lucha contra los delitos informáticos, brindando soluciones cada vez más precisas y robustas para la detección y prevención de estas amenazas (Zhang et al., 2020).

Sin embargo, no todos los algoritmos son igualmente efectivos en todos los contextos de la ciberseguridad. Los estudios han demostrado que algunos algoritmos pueden ser vulnerables a los ataques de adversarios, lo que pone en peligro la eficacia de los sistemas de seguridad basados en aprendizaje automático (Zhang et al., 2020). Por lo tanto, se requiere una evaluación continua y rigurosa de los algoritmos existentes para determinar cuáles son los más aptos para la detección de delitos informáticos en diferentes situaciones.

Por otro lado, en el ámbito del fraude con tarjetas de crédito, la detección y la prevención son tareas desafiantes y que consumen mucho tiempo según Makki et al. (2019). Los algoritmos de aprendizaje automático utilizados para la detección de fraudes deben lidiar con problemas como la clasificación desequilibrada, que ocurre cuando el número de observaciones de la clase minoritaria (fraude) es muy pequeño en comparación con la mayoría (transacciones legítimas) en el conjunto de datos.

Además, Rizvi et al. (2022) expresaron que, en el análisis forense de redes, los algoritmos de aprendizaje automático son una herramienta valiosa para identificar y analizar ataques internos y externos a la red. Sin embargo, la eficacia de estos algoritmos puede verse comprometida por el gran volumen de datos a analizar y la alta frecuencia de falsos positivos generados por los sistemas automatizados.

A lo anterior se le suma que, en el contexto de los delitos cibernéticos más amplios, los algoritmos de aprendizaje automático deben ser capaces de detectar y prevenir una amplia gama de amenazas, desde la pornografía infantil hasta el robo de identidad y el phishing. Los desafíos en este campo incluyen diversidad de las amenazas además de sofisticadas estrategias utilizadas por los ciberdelincuentes, según lo indica Al-Khater et al. (2020).

En vista de estos desafíos, este estudio de Revisión Sistemática de la Literatura (RSL) se centrará en identificar y analizar los algoritmos de aprendizaje automático y aprendizaje profundos más efectivos para la detección de delitos informáticos. A través de este enfoque riguroso y metodológico, se proporciona una comprensión más profunda de las fortalezas y debilidades de estos algoritmos, a mostrar las oportunidades para futuras investigaciones en el campo de la ciberseguridad.

Metodología

Esta investigación constituye una revisión cualitativa sistemática de la literatura (SLR), basada en la metodología de investigación documental. La metodología empleada permitió la consulta de diversas fuentes de información escrita, tales como revistas y libros, entre otras. Se aplicó la investigación descriptiva para detallar los aspectos distintivos del problema de estudio, la investigación cuantitativa para la recolección de datos digitales analizados mediante métodos basados en técnicas matemáticas, estadísticas o informáticas. Además, se incorporó la investigación aplicada, aprovechando los conocimientos adquiridos durante la formación universitaria, integrando la teoría con la realidad para ofrecer soluciones al problema. La ejecución de esta SLR se llevó a cabo siguiendo las etapas de planificación, revisión y análisis, cumpliendo así con el enfoque propuesto.

Planificación

Esta etapa se centra en la formulación de las preguntas de investigación, así como en la especificación de los repositorios de bases de

datos empleados para la búsqueda de artículos científicos y la presentación de los criterios de selección aplicados. El propósito de este estudio es examinar las tendencias en las técnicas de inteligencia artificial para la detección de delitos informáticos. Este objetivo se aborda mediante las siguientes preguntas de investigación:

RQ1. ¿Cuáles son las principales técnicas de la inteligencia artificial utilizadas en la detección de delitos informáticos?

RQ2. ¿Cuál es el nivel de eficiencia de las técnicas de la inteligencia artificial en la detección de delitos informáticos según los resultados obtenidos en casos prácticos?

RQ3. ¿Cómo están evolucionando las técnicas de inteligencia artificial para abordar los desafíos emergentes en ciberseguridad?

Las bases de datos académicas seleccionadas para este estudio son: IEEE Digital Library, Thesai, Redalyc, Scielo y Scopus utilizadas para la recopilación de datos. Se aplicaron diversos términos de búsqueda relacionados con el tema de la investigación, que se combinaron con los operadores booleanos AND y OR. Es importante señalar que las cadenas de búsqueda empleadas variaban según la base de datos o gestor de búsqueda, ya que cada uno tiene un amplio conjunto de documentación (tabla I). Los estudios seleccionados se examinaron y se analizaron en base a criterios de inclusión y exclusión específicos (tabla II).

Esta búsqueda integró estudios primarios publicados entre enero de 2019 y 2023, posteriormente se recogieron los hallazgos de los estudios primarios, como las técnicas de inteligencia artificial que se utilizan en la detección de delitos informáticos y las tendencias actuales en este campo específico. Las preguntas de investigación también sirvieron para identificar los recursos relevantes para la investigación, junto con los datos y las herramientas necesarias para llegar a una conclusión sólida. Al formular preguntas de investigación relevantes y precisas, se puede mejorar la calidad y profundidad de este trabajo científico, resultando en un producto final más informativo. Para facilitar este proceso, se seleccionaron palabras claves relevantes que incluyen: (a) Inteligencia Artificial, (b) Detección de Delitos Informáticos, (c) Ciberseguridad, (d) Algoritmos de Inteligencia Artificial, (e) Aprendizaje Automático y (f) Aprendizaje Profundo.

Cadena de búsqueda base

("Inteligencia Artificial" OR "Algoritmos de IA") AND ("Delitos Informáticos" OR "Ciberseguridad")

Tabla 1

Cadena de búsqueda usada para cada Base de Datos Académica.

Cadena de búsqueda	Bases de Datos Académicas
("Inteligencia Artificial" OR "Aprendizaje Automático") AND "Ciberseguridad"	Redalyc
("Inteligencia Artificial" OR "Algoritmos de IA") AND ("Delitos Informáticos" OR "Ciberseguridad")	Scielo
("Artificial Intelligence Algorithms" OR "Deep Learning Algorithms") AND ("Cybercrime Detection" OR "Cybercrime")	IEEE Digital Library
("Artificial Intelligence" OR "AI Algorithms") AND ("Cybercrime" OR "Cybersecurity")	Thesai
("Artificial Intelligence Algorithms" OR "Machine Learning") AND ("Cybercrime Detection" OR "Cybercrimes")	Scopus

Este protocolo de búsqueda y selección permitió descubrir y seleccionar los documentos más pertinentes para el tema de estudio.

Criterios de selección:

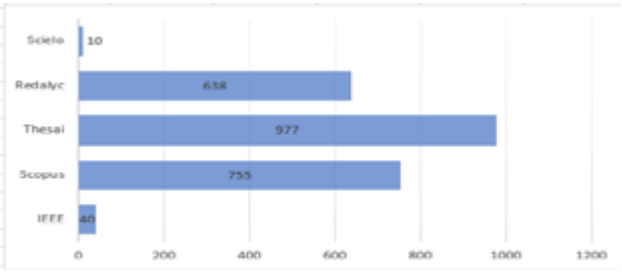
Tabla 2
Criterios de exclusión e inclusión.

Criterios de inclusión	Criterios de exclusión
Documentos donde se utilicen técnicas de inteligencia artificial.	Documentos donde no se utilicen técnicas de inteligencia artificial.
Documentos relacionados con delitos informáticos.	Documentos que no se relacionen con delitos informáticos.
Documentos donde se utilizan métodos/algoritmos para la detección de delitos informáticos.	Tesis sin rigor científico, informes, estudios Duplicados.
Investigaciones relacionadas con las variables de estudio a partir del 2019.	Investigaciones previas al 2019.

Resultados

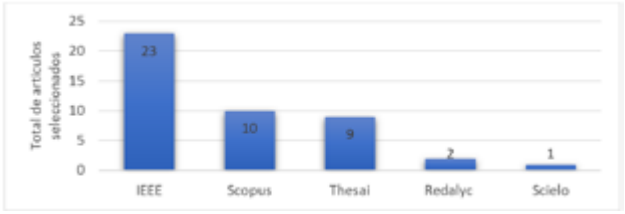
En la etapa inicial de recopilación de datos, se realizó una búsqueda exhaustiva en cinco bases de datos digitales, en esta fase se realiza la búsqueda y selección de los artículos que cumplan con los criterios de inclusión y exclusión; se realizó un análisis del contenido que se encuentra en cada artículo, dando una cifras de 22.536 artículos en la primera búsqueda; después de la utilización de las palabras claves definitivas en base a las preguntas de investigación las cifras resultantes fueron de 2420 artículos (Figura 1).

Figura 1
Artículos encontrados en las distintas bases de datos seleccionadas.



Aunque este conjunto de documentos voluminoso necesitaba un filtrado más riguroso para garantizar que los trabajos seleccionados estuvieran estrechamente relacionados con las tendencias de las técnicas de IA en la detección de delitos informáticos. Este paso fue crucial para mantener la precisión y relevancia del estudio. El efecto de esta filtración es evidente teniendo en total de 45 artículos que cumplen con los criterios mencionados anteriormente.

Figura 2
Artículos seleccionados después de la segunda revisión.



Esta drástica reducción en la cantidad de documentos no es indicativa de una escasez de materiales relevantes, sino más bien una evidencia, por lo tanto, este proceso de búsqueda y selección permitió la identificación de los documentos más adecuados y relevantes para examinar las tendencias actuales en las técnicas de IA aplicadas en la detección de delitos informáticos. A pesar de la disminución en la cantidad de documentos, la relevancia y calidad de los documentos seleccionados proporcionan un buen grupo de evidencias para el análisis posterior.

Dentro del conjunto de 45 documentos analizados, se utilizaron varios algoritmos para identificar y combatir delitos informáticos. Los algoritmos más frecuentemente empleados fueron el SVM (Support Vector Machines), que se obtuvo en 29 documentos, seguido por Naive Bayes en 19 documentos y Random Forest (Bosques Aleatorios) también en 19 documentos, Decision Tree (Árbol de Decisiones) en 18 documentos. Otros algoritmos utilizados fueron KNN (K-Nearest Neighbors) en 17 documentos, Logistic Regression (Regresión Logística) en 13 documentos y CNN (Red Neuronal Convolucional) en 12 documentos. Además, en algunos estudios se aplicaban una combinación de diferentes algoritmos para abordar los delitos informáticos.

Análisis

En este paso, se lleva a cabo la validación de que cada documento seleccionado sea relevante para el tema planteado y que proporciona respuestas a las cuestiones de investigación previamente formuladas. Tras un meticuloso análisis de los documentos escogidos, se procedió a organizar la información para poder

contestar a las interrogantes de investigación. La tabla III recoge la información de los artículos encontrados tomando en cuenta: la base de datos donde fue localizado el artículo, si tiene relación con detección de delitos informáticos, si implementan alguna técnica o algoritmo de clasificación o predicción y Área de Aplicación.

Tabla 3

Fuentes de información de detección de delitos informáticos

	Ítems (Contenido)	Métodos/ Algoritmos	Área de aplicación
Scopus	Otoom et al., 2023, Karim et al., 2023, Wan Ali et al., 2021	SVM, Decision Tree, KNN	Detección de intrusiones, análisis forense
IEEE Digital	Zhang et al., 2020, Makki et al., 2019, Rizvi et al., 2022, Al-Khater et al., 2020, Sun et al., 2021, Halbouni et al., 2022.	KNN, Decision Tree, Random Forest, SVM	Detección de intrusiones, Análisis forense
Thesai		Naive Bayes, Decision Tree, Random Forest	Detección de fraudes, Análisis de malware
Redalyc	Mahfouz et al., 2022, Gawande & Badotra, 2022, Prabha & Kumar, 2022	SVM, Naive Bayes, KNN	Detección de fraudes, Análisis de malware
	Luna-López et al., 2021, Ordoñez-Tumbo et al., 2022		
Scielo	Gil & Anyel, 2021	Algoritmos de aprendizaje automático.	Regulación de la inteligencia artificial (IA)

Nota: Clasificación de estudios primarios seleccionados según el área o sección que abarcan, estas secciones hacen referencia a lo que corresponde a contenido, métodos o algoritmos evaluadas en los estudios y su área de aplicación.

RQ1. ¿Cuáles son las principales técnicas de la inteligencia artificial utilizadas en la detección de delitos informáticos?

En los artículos científicos analizados, se evidencia que la detección de delitos informáticos implica un amplio espectro de técnicas de inteligencia artificial, primordialmente centradas en el aprendizaje automático y el aprendizaje profundo. Por ejemplo, Otoom et al. (2023) propone un marco basado en el aprendizaje automático para identificar nodos influyentes en redes complejas, un enfoque que resulta relevante para la identificación de entidades malintencionadas en escenarios de delitos informáticos. De manera similar, Karim et al. (2023) examinó las principales técnicas de inteligencia artificial utilizadas en la detección de phishing, incluyendo un sistema híbrido de aprendizaje automático que amalgama varias técnicas como Random Forest, Decision Tree, Naive Bayes, K-Nearest Neighbors (KNN) y Support Vector Machine (SVM).

Es importante resaltar que el resto de los trabajos experimentaron con una diversidad de algoritmos alternativos. Esta variedad de técnicas subraya la amplitud del campo de detección de delitos informáticos y sugiere una multitud de enfoques y algoritmos posibles para tratar el problema, dependiendo del contexto y de las características específicas de los datos. La figura 3, generada mediante Wordcloud de RStudio, presenta de forma gráfica el análisis realizado a cada uno de los artículos, visualizando la frecuencia de uso de las distintas técnicas de inteligencia artificial en la detección de delitos informáticos. La elección de utilizar Wordcloud permite una interpretación visual y directa de la relevancia y prevalencia de cada técnica en el campo de estudio.

Figura 3
Wordcloud de los principales algoritmos de la inteligencia artificial en la detección de delitos informáticos.

Tabla 4
Frecuencia de los principales Algoritmos de Inteligencia Artificial

Algoritmos	Total	Algoritmos	Total
SVM	29	RNN	6
Naive Bayes	19	AdaBoost	5
Random Forest	19	J48	5
Decision Tree	18	ANN	4
KNN	17	DNN	4
Logistic Regression	13	XGBoost	4
CNN	12	LSTM	3
K-means	6		

En la Figura 4, también se utilizó la herramienta Wordcloud en RStudio, ilustra las palabras más frecuentes de los temas de los artículos en el campo de estudio relacionado con la inteligencia artificial y la detección de delitos informáticos. La imagen destaca palabras como learning con 25 apariciones, detection con 20 apariciones, machine con 17 apariciones y cybersecurity con 11 apariciones, lo cual subraya la importancia de estas áreas en el campo de investigación. Además de las palabras claves mencionadas, la figura también representa una amplia gama de términos y conceptos que se utilizan en el ámbito de la detección de delitos informáticos, como deep, artificial, classification, ensemble, malicious, malware, entre otros.

La figura 5 además incluye términos específicos como phishing, cyber, intrusion, attack y malware lo cual destaca los diferentes tipos de delitos informáticos que son objeto de estudio y detección mediante técnicas de inteligencia artificial. Además, la presencia de términos como algorithm, neural, network y data enfatiza el papel de la tecnología avanzada en este campo en rápida evolución. En resumen, la tabla 4 ofrece una representación que ilustra la riqueza y complejidad de las palabras más comunes en los temas de la IA en la detección de delitos informáticos, demostrando una amplia gama de técnicas, enfoques, y conceptos que contribuyen al entendimiento y abordaje de este problema multidimensional.

Figura 4
Wordcloud de palabras más frecuentes en los temas de la inteligencia artificial en la detección de delitos informáticos.

Tabla 5
Palabras más frecuentes en los temas de la inteligencia artificial en la detección de delitos informáticos

Palabras	Frecuencia	**Palabras**	**Frecuencia**
Learning	25	Cyber	4
Detection	20	Framework	3
Machine	17	Security	3
Using	12	Study	3
Cybersecurity	11	Cybercrime	3
Based	10	Attacks	3
Deep	9	URL	3
Intelligence	8	Attack	3
System	7	Intrusion	3

Artificial	6	Model	3
Classification	5	Science	3
Ensemble	5	Malicious	3
Data	4	Malware	3
Survey	4	Cyber	4
Techniques	4	Framework	3
Network	4	Security	3
Detecting	4	Study	3
phishing	4	Cybercrime	3
Journal	4	Attacks	3

RQ2. ¿Cuál es el nivel de eficiencia de las técnicas de la inteligencia artificial en la detección de delitos informáticos según los resultados obtenidos en casos prácticos?

El nivel de eficiencia de las técnicas de inteligencia artificial en la detección de delitos informáticos, reflejado en casos prácticos, se puede visualizar en la tabla 6. Esta tabla recopila los resultados de varios estudios, mostrando métricas claves como la exactitud y la precisión. Estos resultados indican que las técnicas de inteligencia artificial son altamente eficientes en la detección de delitos informáticos, con una exactitud y precisión cercanas al 100% en todos los casos. La tabla 6 muestra la eficiencia de diferentes técnicas de inteligencia artificial utilizadas en la detección de delitos informáticos.

Tabla 6

Nivel de eficiencia de las técnicas de inteligencia artificial

Artículos	**Algoritmos**	**Exactitud%**	**Precisión%**
Un estudio experimental con enfoques de clasificación desequilibrados para la detección de fraudes con tarjetas de crédito.	C5.0	96%	0,6%
	SVM	96%	0,63%
	ANN	96%	0,61%
	Logistic Regression	96%	0,66%
	Naive Bayes	93%	0,5%
	BBN	94%	0,64%
	KNN	95%	0,29%
	NSA	92%	0,29%
Evaluación de las características del conjunto de datos de ciberseguridad para su aplicabilidad a algoritmos de redes neuronales que detectan anomalías de ciberseguridad.	Decision Tree	89,86%	N/A
	J48	99,94%	N/A
	FFNN	98,8%	N/A
	RNN	99,88%	N/A
Aprovechar las técnicas de aprendizaje automático para identificar documentos señuelo engañosos asociados con ataques de correo electrónico dirigidos.	Random Forest	64%	0,66%
	SVM	70,5%	0,708%
	KNN	64%	0,621%
	MLP	69%	0,963%
	Decision Tree	69%	0,67%
Enfoques de aprendizaje automático y aprendizaje profundo para la ciberseguridad: una revisión.	SVM	82,37%	0,74%
	KNN	85,2%	N/A
	ANN	98,32%	N/A
	K-means	90%	N/A
	CNN	97,52%	N/A
	RNN	96,7%	N/A

Sistema de detección de phishing mediante híbrido. Aprendizaje automático basado en URL.	Random Forest	96,77%	0,967%
	Decision Tree	95,41%	0,96%
	Naive Bayes	88,39%	0,95%
	KNN	58,63%	0,689%
	SVM	71,86%	0,96%
Prototipo Cross Platform Orientado a Ciberseguridad, Conectividad Virtual, Big Data y Control de Inteligencia Artificial.	XGBoost	99,99%	0,99%
	Random Forest	99,88%	0,99%
	CNN	99,65%	0,988%
SeFACED: análisis forense basado en la semántica y clasificación de datos de correo electrónico mediante aprendizaje profundo.	Logistic Regression	99,53%	0,997%
	Nearest Neighbors	99,65%	0,997%
	SVM	99,53%	0,997%
	Logistic Regression	91%	0,96%
	SVM	90%	0,91%
	SGD	87%	0,89%
	Naive Bayes	90%	0,91%
	Random Forest	90%	0,92%
	LSTM	93%	0,93%
Sistema inteligente de monitoreo para condiciones ambientales en Industria 4.0	J48	99,86%	N/A
	Random Forest	99,31%	N/A
	Random Tree	95,07%	N/A
Un nuevo marco basado en aprendizaje automático para detectar el discurso de odio religioso árabe en las redes sociales.	SVC	78%	0,78%
	PAC	73%	0,73%
	KNN	70%	0,73%
	Logistic Regression	73%	0,73%
	Naive Bayes	72%	0,73%
Detección avanzada de ataques de amenazas persistentes mediante algoritmos de agrupación.	Decision Tree	94%	0,799%
	Random Forest	99%	0,999%
	SVM	96%	0,853%
	KNN	97%	0,888%
Modelo de conjunto para sistema de detección de intrusiones en la red basado en embolsado utilizando J48.	J48	81,74%	0,8580%
	KNN	78,29%	0,836%
	SVM	75,39%	0,8020%
	Random Forest	80,45%	0,85%
	Naive Bayes	76,12%	0,81%
Clasificación de nombres de dominio maliciosos COVID-19	DTC	93,1%	0,8137%
	RFC	96,26%	0,9032%
	GBM	97,01%	0,9536%
	XGBoost	96,59%	0,9182%
	SVM	96,89%	0,9587%
	MLP	96,53%	0,9557%
Técnicas de aprendizaje automático para detectar ataques de URL de phishing.	AdaBoost	95,43%	0,957%
	NN	90,23%	0,8683%
	Naive Bayes	92,27%	0,9254%
Una visión de la detección de malware sin archivos basada en aprendizaje automático.	Random Forest	N/A	0,875%
	SVM	N/A	0,75%
	Logistic Regression	N/A	0,25%
	XGBoost	N/A	0,75%
	KNN	N/A	0,375%

Clasificación inteligente de ciberseguridad utilizando la optimización del juego del caos con un modelo de aprendizaje profundo.	KNN	98,57%	N/A
	Random Forest	99,47%	N/A
	Decision Tree	99,8%	N/A
	SVM	89,18%	N/A
	Naive Bayes	92,12%	N/A
	ICC-CGODL	99,72%	N/A
Ensem_SLDR: Clasificación del Cibercrimen utilizando la técnica de aprendizaje conjunto.	Hybrid Model	96,55%	1%
	Voting Ensemble	94,83%	0,95%
	XGBoost	87,93%	0,91%
	Gradient Boosting	93,1%	0,95%
	AdaBoost	93,1%	0,95%
Implementación de optimización de hiperparámetros y sobre muestreo en la detección de ciberacoso mediante un enfoque de aprendizaje automático.	Linear Support Vector Classifier	97,38%	0,9924%
Un novedoso sistema de predicción de pistas de ciberataques que utiliza el modelo R2CNN en cascada.	LSTM	99%	N/A
	LSTMCNN	90,88%	N/A
	GBR-RF	99%	N/A
	CR2CNN	99,2%	N/A
Predicción de software malicioso en entornos de IoT basado en técnicas de aprendizaje automático y minería de datos.	Decision Tree	95,67%	0,958%
	Random Forest	98,48%	0,9855%
	KNN	96,48%	0,977%
	SVM	98,48%	0,9845%
	Naive Bayes	94,79%	0,9668%
Eth-PSD: un enfoque de detección de estafas de phishing basado en aprendizaje automático en Ethereum.	J48	96,34%	0,96%
	Decision Tree	96,36%	0,96%
	Jrip	90,65%	0,91%
	KNN	97,76%	0,97%
	Naive Bayes	95,28%	0,95%
	OneR	92,42%	0,92%
	Part decision List	90,09%	0,91%
	Fast Decision Tree	96,1%	0,96%
Sistema computacional para clasificar delitos cibernéticos mediante aprendizaje automático.	LinearSvc	99,23%	N/A
	Logistic Regression	99,38%	N/A
	MultinomialNB	98,95%	N/A
	Random Forest	88,69%	N/A
Enfoque de aprendizaje profundo para la detección eficiente del parpadeo con concepto de optimización híbrida.	CNN+BI-LSTM	88%	0,88%
	C-LSTM	86,5%	0,865%
	Bi-LSTM	86,5%	0,865%
	RNN	85,5%	0,855%
	CNN	88%	0,88%
Un sólido método de detección de falsificaciones para ataques de copiar, mover y empalmar en imágenes.	LBP	92,18%	N/A
	DCT	95,84%	N/A
Un motor de secuenciación de ADN digital para la detección de ransomware mediante aprendizaje automático.	Naive Bayes	78,5%	N/A
	Decision Stump	75,8%	N/A
	AdaBoost	83,2%	N/A
	DNAct-Ran	87,9%	N/A

Detección de fraude con tarjetas de crédito mediante algoritmos de aprendizaje automático y aprendizaje profundo de última generación.	CNN	96,34%	N/A
	BL	99,72%	N/A
	Random Forest	99,92%	N/A
	SVM	99,93%	N/A
	KNN	99,91%	N/A
	Decision Tree	99,93%	N/A
	Logistic Regression	99,91%	N/A
Robusta detección inteligente de malware mediante aprendizaje profundo.	CNN	98,8%	0,997%
	LightGBM	97,5%	0,99%
	Logistic Regression	54,9%	0,526%
	Naive Bayes	53,8%	0,52%
	KNN	95,1%	0,955%
	Decision Tree	96,9%	0,971%
	AdaBoost	83%	0,861%
	Random Forest	97%	0,986%
	SVM	96,1%	0,964%
	DNN	98,9%	0,997%
Detección de URL maliciosas basada en un modelo de articulación neuronal paralela.	CNN	99,56%	0,9975%
	LSTM	99,55%	0,9978%
	CapstNet	99,72%	0,995%
	Bi-LSTM	99,68%	0,9976%
	Bi-IndRNN	99,68%	0,9943%
	CNN+LSTM	99,68%	0,9943%
Suficiencia del aprendizaje automático conjunto Métodos para la detección de sitios web de phishing.	K-means	62,6%	0,5167%
	SVM	75,46%	0,673%
	Naive Bayes	83,85%	0,8798%
	KNN	86,95%	0,8172%
	Logistic Regression	89,76%	0,8738%
	LDA	91,54%	0,8277%
	CART	95,16%	0,9301%
	Random Forest	97,01%	0,9544%

En la tabla 6, presentan una recopilación de estudios que se centran en la detección de delitos informáticos utilizando diferentes algoritmos de aprendizaje automático y profundo. Cada estudio se evalúa en términos de su precisión y exactitud. En términos de exactitud, varios algoritmos también demostraron un rendimiento impresionante. Algunos de ellos, como Decision Tree, Random Forest, SVM y ANN, alcanzan valores cercanos o superiores al 95%. Estos algoritmos pueden ser considerados como opciones sólidas para trabajos futuros, especialmente en escenarios donde la exactitud es crucial para una detección precisa de delitos informáticos.

Por otro lado, en términos de precisión, se destaca que algunos algoritmos alcanzan valores muy altos, como es el caso de XGBoost, Random Forest, CNN, LSTM, entre otros, que obtienen valores cercanos a 0,99 o incluso superiores en algunas situaciones específicas. Estos algoritmos son altamente recomendables para aplicaciones donde la precisión es un factor crítico en la detección de delitos informáticos. Dado que los resultados varían según el conjunto de datos y el tipo de delito informático, es recomendable que futuros trabajos en este campo consideren la utilización de conjuntos de datos más diversos y equilibrados para obtener conclusiones más sólidas y generalizables.

593 Digital Publisher CEIT ISSN 2588-0705

RQ3. ¿Cómo están evolucionando las técnicas de inteligencia artificial para abordar los desafíos emergentes en la ciberseguridad?

Las técnicas de IA están evolucionando para enfrentar desafíos emergentes en la ciberseguridad, abordando aspectos como la privacidad de los datos, la eficiencia en la detección de amenazas y la adaptabilidad frente a tácticas de ataque nuevas y cambiantes.

Ch et al. (2020), se propone un sistema que utiliza el aprendizaje automático para clasificar los delitos cibernéticos. El sistema se basa en un conjunto de datos de casos de delitos cibernéticos que han sido clasificados manualmente por expertos. Dicho sistema es capaz de lograr una alta precisión en la clasificación de delitos cibernéticos. También se discuten los desafíos de clasificar los delitos cibernéticos y el potencial del aprendizaje automático para abordar estos desafíos.

En consecuencia, se muestra que todas las metodologías se basan principalmente en la toma de decisiones, como la detección de delitos informáticos a través de datos recopilados y analizados utilizando técnicas de inteligencia artificial. Todos los estudios están enfocados en la identificación y prevención de delitos informáticos, buscando la seguridad de las infraestructuras digitales y la protección de la información personal y corporativa. Lo más importante es saber qué algoritmos y técnicas de inteligencia artificial son más efectivos y cómo se pueden implementar para minimizar el impacto de los delitos informáticos. La tabla 7 presenta un resumen de los artículos analizados para responder a esta pregunta de investigación.

Discusiones

Esta revisión sistemática de la literatura finalizó con 45 artículos relevantes, lo que demostraron cómo la investigación en este campo está creciendo gradualmente con el paso del tiempo. Los resultados refuerzan la importancia crítica de mejorar la detección y prevención de delitos informáticos mediante el uso de técnicas de inteligencia artificial. Durante el proceso de investigación, se demostró que la mayoría de los estudios utilizaron varios tipos de algoritmos de inteligencia artificial. Los más frecuentemente utilizados incluyen SVM, Decision Tree, Logistic Regression, Naive Bayes, KNN y Random Forest. Dentro de este marco, tanto XGBoost, Random Forest y Logistic Regression han demostrado un notable equilibrio entre precisión y exactitud en múltiples investigaciones, lo que los convierte en opciones sobresalientes. Sin embargo, es fundamental tener en cuenta que la elección del algoritmo debe ajustarse según el conjunto de datos y el contexto específico. Por lo tanto, se sugiere llevar a cabo pruebas preliminares y definiciones para determinar cuál de ellos se adecua mejor a la necesidad en particular.

Tabla 7

Investigación sobre la detección de delitos informáticos utilizando técnicas de inteligencia artificial

Estudio de caso / Artículo / Investigación	Descripción del problema	Delitos Informáticos	Base de Datos	Técnicas de Inteligencia Artificial
Ensemble Model for Network Intrusion Detection System Based on Bagging Using J48	Detección de ataques a la red.	Ataque de denegación de servicio (DoS)	Scopus	Decision Tree J48 KNN SVM Random Forest NB
A Machine Learning Based Framework for Identifying Influential Nodes in Complex Networks	Dificultad de medir la importancia funcional de los nodos en redes complejas debido a la existencia de una relación compleja y no lineal.	Ataques de denegación de servicio (DDoS)	IEEE	Naive Bayes Decision Tree SVM KNM Logistic Regression K-Core MLP
A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View	Seguridad de los algoritmos de aprendizaje automático y sus datos de entrenamiento frente a diversas amenazas	N/A	IEEE	Naive Bayes Decision Tree SVM Logistic Regression Clustering DNNs PCA/LASSO
An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection	Detección de fraudes en tarjetas de crédito, específicamente el desafío de la clasificación desequilibrada	Robo simple Fraude de solicitud, Fraude de bancarrota, Fraude interno, Fraude de falsificación	IEEE	C5.0 SVM ANN Logistic Regression Naive Bayes BBN KNN NSA
Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions	Desafíos y limitaciones de la informática forense de redes	DDoS, DoS, Fuerza bruta Botnets, Ataques web	IEEE	Neural Networks Naive Bayes Decision Trees Random Forest SVM Hierarchical clustering K-means DBSCAN CNN RNN
Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature	Falta de una revisión sistemática y completa de los métodos de inteligencia artificial (IA) para combatir los delitos informáticos.	Malware, Ransomware	IEEE	Naive Bayes Decision Trees SVM K-means ANN KNN CNN Randon forest AdaBoost Q-Learning
Comprehensive Review of Cybercrime Detection Techniques	La necesidad de detectar y prevenir eficazmente los delitos informáticos	Ciberespionaje, Ciberguerra, Pornografía, infantil, Ciberacoso, Ciberterrorismo	IEEE	Naive Bayes Decision Trees J48 SVM K-Means Logistic Regression KNN

Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies	Detección de intrusiones en el campo de la ciberseguridad	Ataques de denegación de servicio (DoS), Phishing, Malware	IEEE	Decision Trees Decision Trees Decision Trees J48 FFNN RNN ANN DNN CNN
Explainable Artificial Intelligence in CyberSecurity: A Survey	La falta de transparencia en los sistemas de Inteligencia Artificial (IA) y su aplicación en el campo de la ciberseguridad	Phishing, Cryptojacking, malware	IEEE	CNN RNN SVM Decision Trees Bosques aleatorios DBSCAN K-means GRID Algoritmo de agrupamiento jerárquico MODEL PARTITION DENSITY
Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity	El creciente número de amenazas cibernéticas y la sofisticación de las técnicas utilizadas por los ciberdelincuentes.	Ataques de denegación de servicio (DoS)	IEEE	Random Forest DDoS SVM
Leveraging Machine Learning Techniques to Identify Deceptive Decoy Documents Associated With Targeted Email Attacks	Detección y prevención de ataques de correo electrónico dirigidos.	Spear phishing	IEEE	Random Forest SVM KNN MLP Decision Trees
Machine Learning and Deep Learning Approaches for CyberSecurity: A Review	El desarrollo de un sistema de detección de intrusiones efectivo para proteger los datos en el contexto de los crecientes y cambiantes ataques cibernéticos	Ataques de denegación de servicio (DoS)	IEEE	Naive Bayes CNN DNN Random Forest SVM
Machine Learning and Deep Learning Methods for Cybersecurity	Detección de intrusiones en redes	Ataques de denegación de servicio (DoS)	IEEE	SVM KNN ANN K means CNN RNN
Phishing Detection System Through Hybrid Machine Learning Based on URL	Prevalencia de los ataques de phishing	spear phishing, phishing	IEEE	Random Forest Decision Tree Naive Bayes KNN SVM
Prototype Cross Platform Oriented on Cybersecurity, Virtual Connectivity, Big Data and Artificial Intelligence Control	Efectividad en prototipo de plataforma cruzada basado en la ciberseguridad, la conectividad virtual.	ataques de denegación de servicio (DDoS), Phishing, Malware, robo de identidad	IEEE	XGBoost Random Forest Convolutuinal Neural Network Logistic Regression Nearest Neighbors SVM
SeFACED: Semantic-Based Forensic Analysis and Classification of E-Mail Data Using Deep Learning	El análisis proactivo de datos para prevenir ciberataques y crímenes en el contexto de la creciente cantidad de datos generados por dispositivos IoT y el uso extensivo del correo electrónico.	Disrupción de operaciones y servicios mediante ataques a dispositivos IoT, Ciberataques spoofing, phishing, bombardeo de correo, whaling y spamming	IEEE	Logistic Regression SVM SGB NB Random Forest LSTM
Sistema inteligente de monitoreo para condiciones ambientales en Industria 4.0	La necesidad de monitorear las condiciones ambientales en la industria, especialmente en ambientes donde se emplean motores.	Ataques a dispositivos IoT, Malware	Redalyc	J.48 Random Forest Random Tree

An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT	La seguridad en el contexto del Internet Industrial de las Cosas (IIoT).	Ataques a dispositivos IoT, Malware	Redalyc	SVM
An Empirical Study on Fake News Detection System using Deep and Machine Learning Ensemble Techniques	Propagación de noticias falsas y desinformación a través de diversas plataformas de redes sociales	Difusión de noticias falsas, Manipulación de imágenes o videos	Thesai	Naive Bayes Decision Tree Random Forest SVM KNN Logistic Regression CNN RNN
A Novel Machine Learning-based Framework for Detecting Religious Arabic Hatred Speech in Social Networks	Transfer Learning (TL)	Hacking, Fraude en línea, Malware, Robo de datos	Thesai	SVC Related work
Advanced Persistent Threat Attack Detection using Clustering Algorithms	La detección efectiva de los ataques de Amenaza Persistente Avanzada (APT)	Ataques de denegación de servicio (DoS).	Thesai	Decision Tree Random Forest SVM KNN
Phishing or Not Phishing? A survery on the Detection of Phishing Website	Métodos utilizados para detectar sitios web de phishing	Detención de Phishing	IEEE	SVM Random Forest Logistic Regression Naive Bayes Decision Tree XGBoost CNN
COVID-19 malicious domain names classification	El aumento de los delitos informáticos, especialmente en el contexto de la pandemia de COVID-19.	Phishing	Scopus	DTC RFC GBM XGBoost SVM MLP
Machine Learning Techniques for Detecting Phishing URL Attacks	La prevalencia de los ataques de phishing, que son un tipo de delito informático en el que los usuarios son engañados para revelar su información privada al seguir enlaces a sitios web ilegales.	Phishing	Scopus	SVM DNN GA Redes neuronales de autoestructuración con un tipo de red neuronal artificial Naive Bayes
An Insight into the Machine-Learning-Based Fileless Malware Detection	La aparición del malware sin archivo (fileless malware), lo cual ha cambiado el panorama del desarrollo de malware.	Malware	Scopus	Random Forest SVM Logistic Regression GB Decision Tree XGB KNN
Android Malware Detection Using ResNet-50 Stacking	La creciente amenaza del malware móvil, específicamente dirigido al sistema operativo Android.	Malware	Scopus	ResNet-50 SVM
Intelligent Cybersecurity Classification Using Chaos Game Optimization with Deep Learning Model	El aumento de los ciberataques y la necesidad de desarrollar métodos efectivos para la detección y clasificación de estos ataques en el campo de la ciberseguridad	Robo de identidad, Malware, Phishing	Scopus	KNN Random Forest Decision Tree SVM Naïve Bayes ICC-CGODL
Ensem_SLDR: Classification of Cybercrime using Ensemble Learning Technique	La clasificación de delitos informáticos en dos secciones, 66 y 67, de la Ley de Tecnología de la Información de 2000 en la India.	Phishing, malware	Scopus	Hybrid Model Voting Ensemble XGBoost Gradient Boosting AdaBoost

IMPLEMENTATION OF HYPERPARAMETER OPTIMISATION AND OVER-SAMPLING IN DETECTING CYBERBULLYING US-ING MACHINE LEARN-ING APPROACH	La detección de ciberacoso (cyberbullying) en las redes sociales	Ciberacoso	Scopus	SVM
A Novel Cyber-Attack Leads Prediction System using. Cascaded R2CNN Model	La detección de ciberataques en dispositivos IoT conectados a Internet	Software malicioso, piratería informática debido al acceso no autorizado, Hombre en el medio	Thesai	LSTM LSTMCNN GBR-RF CR2CNN
Predicting Malicious Soft-ware in IoT Environment Based on Machine Learning and Data Mining Techniques	La seguridad de los dispositivos de Internet de las cosas (IoT) y la detección de software malicioso en un entorno de IoT.	ataques de denegación de servicio distribuido (DDoS) Ciberespionaje Ataques de botnets de IoT	Thesai	DT RF KNN SVM NB
Eth-PSD: A Machine Learn-ing-Based Phishing Scam Detection Approach in Ethereum	El rápido crecimiento de los delitos cibernéticos en la plataforma Ethereum, especialmente las estafas de phishing.	Estafas de phishing, Carteras de estafa, Esquemas Ponzi	IEEE	j48 Decision tree Jrip KNN Naive Bayes OneR Part decision List Fast Decision Tree
BCT-CS: Blockchain Tech-nology Applications for Cyber Defense and Cyberse-curity: A Survey and Solutions	La creciente amenaza de los ciberdelitos y la necesidad de una defensa cibernética efectiva.	Ataques de denegación de servicio (DoS), Ataques de hombre en el medio (MitM), Ataques de phishing	Thesai	NA
Computational System to Classify Cyber Crime Offenses using Machine Learning	La falta de un marco generalizado para categorizar los delitos cibernéticos mediante la extracción de características de los casos.	Descarga ilegal Piratería de libros de texto, Descarga ilegal de aplicaciones Software pirateado, Descarga ilegal de música Hackeo de la comunicación de una planta de energía Hackeo de teléfonos inteligentes, Hackeo de sitios web gubernamentales, Robo de información de tarjetas de crédito, Robo de identidad	IEEE	LinearSvc Logistic Regression MultinomialNB Random Forest
Deep-Learning Approach for Efficient Eye-blink Detection with Hybrid Opti-mization Concept	El desarrollo de un modelo de detección de parpadeo de ojos eficiente utilizando un enfoque de aprendizaje profundo (deep learning).	N/A	Thesai	CNN+BI-LSTM C-LSTM Bi-LSTM RNN C NN
A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images	La detección de falsificaciones en imágenes, específicamente los ataques de copia-movimiento y empalme.	Difusión de imágenes falsas para alterar los procesos operativos y de toma de decisiones	Scopus	LBP DCT SVM
Cybercrime: Identifica-tion and Prediction Using Machine Learning Techniques	La identificación y predicción de delitos cibernéticos utilizando técnicas de aprendizaje automático.	Robo de identidad sintético, Intrusión en la red, Fraude con tarjetas de crédito	Scopus	GMM SVM
Anomaly-based Network Intrusion Detection using Ensemble Machine Learning Approach	El diseño de un Sistema de Detección de Intrusiones (IDS) basado en clasificadores de Aprendizaje Automático (Machine Learning) y la evaluación de su rendimiento utilizando el conjunto de ataques del dataset UNSW-NB15.	Denial-of-Service (DDoS), Man-In-The-Middle (MITM), Malware, Cross-Site, Scripting (XSS), Escuchas telefónicas	Thesai	Ensemble Machine Learning Algoritmo de agrupación de picos de densidad modificada y redes de creencias profundas

Toward A Holistic, Efficient, Stacking Ensemble Intrusion Detection System using a Real Cloud-based. Dataset	La detección de intrusiones eficiente y holístico utilizando un conjunto de datos en la nube real.	Ataques de denegación de servicio (DoS)	Thesai	Redes neuronales K means Decision Tree Regresión logística SVM Naive Bayes
Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad	Desafíos que plantea la regulación jurídica de la inteligencia artificial (IA).	Retos de regular los sistemas de aprendizaje automático	Scielo	Algoritmos de aprendizaje automático
A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning	Se propone DNAact-Ran, un motor de secuenciación de ADN digital para la detección de ransomware mediante el aprendizaje automático	Ransomware	IEEE	Naive Bayes Decision Stump AdaBoost DNAct-Ran
Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	Detección de fraudes con tarjetas de crédito utilizando algoritmos de aprendizaje automático y aprendizaje profundo. El fraude con tarjetas de crédito es un problema significativo que afecta tanto a los titulares de tarjetas como a las compañías financieras.	Robo simple Fraude de solicitud, Fraude de bancarrota, Fraude interno, Fraude de falsificación	IEEE	CNN BL Random Forest SVM KNN Decision tree Logistic Regression
Robust Intelligent Malware Detection Using Deep Learning	Se plantea una preocupación significativa para la seguridad. Las soluciones actuales de detección de malware basadas en análisis estáticos y dinámicos de firmas y patrones de comportamiento son ineficaces para identificar malwares desconocidos en tiempo real.	Malware Software malicioso	IEEE	CNN LightGBM Logistic Regression Naive Bayes KNN Decision tree AdaBoost Random Forest SVM DNN
Sufficiency of Ensemble Machine Learning Methods for Phishing Web-sites Detection	Detección eficiente de sitios web de phishing, El estudio busca comparar el rendimiento de varios métodos de aprendizaje automático y aprendizaje profundo para encontrar la solución más adecuada para la clasificación binaria de phishing en entornos de entrenamiento actualizados y detección en tiempo real.	Los métodos discutidos en el artículo pueden ayudar a defender contra el delito informático de phishing. El phishing es una técnica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener acceso a información sensible, como contraseñas, números de tarjetas de crédito y datos bancarios.	IEEE	K-means SVM Naive Bayes KNN Logistic Regression LDA CART Random Forest
Malicious URL Detection Based on a Parallel Neural Joint Model	Detección eficiente de URL maliciosas, que son enlaces diseñados para engañar a los usuarios y dirigirlos a sitios web fraudulentos o infectados con malware. La detección precisa de estas URL es esencial para proteger a los usuarios y sistemas contra amenazas en línea.	Se propone un algoritmo de modelo conjunto neural paralelo para detectar URL maliciosas basado en la extracción de información semántica y visual. Se enfoca en capturar vectores multimodales de información visual y semántica de manera sincrónica para mejorar la precisión en la detección de URL maliciosas.	IEEE	CNN LSTM CapstNet Bi-LSTM Bi-IndRNN CNN+LSTM

Se observa que se ha empleado varias técnicas de inteligencia artificial en la detección de delitos informáticos. Estas técnicas se aplican principalmente para detectar una amplia gama de delitos cibernéticos, incluyendo ataques de denegación de servicio (DoS), malware, ransomware, detección de intrusiones en sistemas, phishing y fraude.

En un estudio realizado por Wan Ali et al. (2021), se destacó la aplicación de la optimización de hiperparámetros y sobre muestreo en la detección de ciberacoso, usando un enfoque de aprendizaje automático, proporcionando resultados significativos en términos de precisión y detección. Para visualizar de forma más intuitiva la frecuencia de uso de cada técnica, se empleó la herramienta Wordcloud de RStudio. Este análisis reveló que SVM es la técnica más utilizada, con apariciones en 29 trabajos, seguida de Naive Bayes y Random Forest (19 trabajos), Decision Tree (18 trabajos) y KNN (17 trabajos). Otras técnicas como Logistic Regression, CNN, RNN, ANN, entre otras, fueron también empleadas, aunque con menor frecuencia.

Para ilustrar, el estudio realizado por Sun et al. (2021) emplearon el algoritmo de aprendizaje automático Random Forest para la clasificación de documentos, logrando identificar correctamente documentos engañosos con una exactitud notable del 99.7%. Este caso ilustra el potencial de eficiencia que la inteligencia artificial puede alcanzar en la detección de delitos informáticos.

Por otro lado, Halbouni et al. (2022) utilizaron el algoritmo Naive Bayes para la detección de intrusiones y obtuvo una exactitud del 81.9%. Además, emplearon el algoritmo Random Forest para la misma tarea, alcanzando una exactitud impresionante del 99.9%. También utilizó SVM para la detección de intrusiones y obtuvo una exactitud del 92.9%. Luego, empleó las Redes Neuronales Profundas (DNN) para la detección de intrusiones y obtuvo una exactitud del 78.9%. Otro estudio aplicó las Redes Neuronales Convolucionales (CNN) para la detección de malware, logrando una exactitud del 97.6%.

Estos resultados evidencian que las técnicas de inteligencia artificial pueden ser muy eficaces en la detección de delitos informáticos. No obstante, es importante señalar que la eficacia de estas técnicas puede variar dependiendo de la naturaleza de los datos y la configuración específica del algoritmo. La eficiencia de las técnicas de inteligencia artificial en la detección de delitos informáticos también se demostró en el estudio realizado por Larriva-Novo et al. (2020). En este estudio, se emplearon diferentes algoritmos, obteniendo los siguientes resultados: (a) Algoritmo de Red Neuronal Profunda (DNN) con exactitud de 99.87% y precisión del 0.998%. (b) Algoritmo de Red Neuronal Convolucional (CNN) con exactitud de 99.89% y precisión del 0.998%. (c). Algoritmo de Red Neuronal Recurrente (RNN) con exactitud de 99.88% y precisión del 0.998%

Liu et al. (2018), destacan la relevancia de la criptografía y la privacidad diferencial en la protección de los datos, a pesar de su complejidad y costos asociados. Asimismo, apunta al valor de la encriptación homomórfica y del aprendizaje profundo seguro. Este trabajo recuerda que, a pesar de los retos en términos de complejidad y costos, las soluciones criptográficas y de privacidad diferencial son esenciales en la lucha constante por la seguridad de los datos. Wiafe et al. (2020), señalan la creciente adopción de técnicas de aprendizaje profundo y aprendizaje automático para enfrentar varios desafíos de ciberseguridad, como la detección de malware y la predicción de amenazas. En este trabajo se subraya cómo las técnicas de aprendizaje automático y aprendizaje profundo están demostrando su valía al abordar con éxito una variedad de problemas de ciberseguridad.

Larriva-Novo et al. (2020), enfatizan la necesidad de optimizar los algoritmos de IA para mejorar la detección de amenazas cibernéticas, y la importancia de utilizar conjuntos de datos más amplios y diversos. Larriva-Novo et al. (2020), apuntan a una realidad clave de la ciberseguridad en la era de la IA: la eficacia de nuestras herramientas depende tanto de la calidad del algoritmo como de la diversidad y amplitud de los datos que se utilizan para entrenarlas. Existen

trabajos en los que se destaca la adaptabilidad de la IA frente a nuevas tácticas de ataque, el nivel de automatización para la detección y respuesta a amenazas, y la capacidad para analizar grandes volúmenes de datos. Massaro et al. (2020) subraya cómo la IA, a través de su adaptabilidad, automatización y habilidades analíticas, puede ayudar a anticipar y responder a las amenazas en el cambiante panorama de la ciberseguridad. (Massaro et al., 2020).

Se puede indicar que existe un aumento en la utilización de técnicas de inteligencia artificial más complejas, como el aprendizaje profundo (Deep Learning). Los modelos como las Redes Neuronales Convolucionales (CNN) y las Redes Neuronales Recurrentes (RNN) se utilizan cada vez más, lo que indica un cambio hacia técnicas más avanzadas en la detección de delitos cibernéticos. En cuanto a los delitos, los ataques de denegación de servicio (DoS), el phishing y el malware parecen ser los delitos más frecuentes en los que se emplean las técnicas de inteligencia artificial para su detección. Sin embargo, también se utilizan estas técnicas para detectar otros delitos como la difusión de noticias falsas, la suplantación de identidad y el ciberacoso.

Para futuros trabajos, hay varias oportunidades prometedoras: a) Uso de técnicas avanzadas de inteligencia artificial: A medida que las técnicas de inteligencia artificial evolucionan, se hace necesario explorar más en el uso de técnicas avanzadas como el aprendizaje profundo y el aprendizaje por refuerzo para mejorar la detección de delitos informáticos. Estos modelos son capaces de extraer características de alto nivel y manejar datos no estructurados de manera más eficiente, lo que puede mejorar el rendimiento de los sistemas de detección. b) Soluciones de IA específicas para tipos de delitos: El desarrollo de soluciones de inteligencia artificial específicas para ciertos tipos de delitos puede ser un enfoque prometedor.

Conclusiones

Se puede concluir que el Ataque de Denegación de Servicio (DoS) es el delito informático más recurrentemente abordado en estos estudios, seguido por problemas asociados al Phishing y al Malware. Esta tendencia refleja las amenazas más destacadas en el ámbito de la seguridad cibernética, subrayando la necesidad de una mayor innovación y atención en estas áreas específicas. En relación con las bases de datos utilizadas, destaca que los estudios de IEEE y Scopus son los más prevalentes, lo cual puede indicar la calidad y profundidad de la investigación, al tratarse de fuentes académicas bien reconocidas.

Respecto a la evolución de las técnicas de inteligencia artificial para abordar los desafíos emergentes en ciberseguridad, es claro que la Inteligencia Artificial desempeñará un papel crucial en la lucha contra los delitos informáticos. Se necesita un enfoque más integrado que combine diversos algoritmos de IA para hacer frente de manera efectiva a las amenazas cibernéticas. Dado que los delitos informáticos están en constante evolución, resulta imperativo que la investigación en este campo se mantenga al día con estas tendencias. Una posible dirección para investigaciones futuras sería el desarrollo de sistemas de IA capaces de aprender y adaptarse dinámicamente a nuevas amenazas, empleando algoritmos de aprendizaje profundo y aprendizaje automático, junto con técnicas de aprendizaje por refuerzo para mejorar el rendimiento de los sistemas con el tiempo.

Considerando el impacto social, es esencial llevar a cabo más investigaciones sobre la detección y prevención de delitos cibernéticos que afectan directamente a los individuos, como el ciberacoso, el robo de identidad y la difusión de noticias falsas. En este contexto, la IA puede contribuir no solo a la seguridad cibernética de las organizaciones, sino también a la protección individual en la era digital. Por ende, la inteligencia artificial ofrece una oportunidad única para avanzar en la detección y prevención de delitos informáticos. No obstante, es fundamental que los investigadores, los profesionales de la seguridad y las partes interesadas de la industria continúen colaborando y compartiendo conocimientos para

abordar estos desafíos y maximizar el potencial de estas tecnologías.

Referencias Bibliográficas

Advanced Persistent Threat Attack Detection using Clustering Algorithms—ProQuest. (2022). Recuperado 6 de septiembre de 2023, de https://www.proquest.com/openview/e4cf78c9c76360df56db08e93dac95b2/1?pq-origsite=gscholar&cbl=5444811.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8, 137293-137311. https://doi.org/10.1109/ACCESS.2020.3011259

An Empirical Study on Fake News Detection System using Deep and Machine Learning Ensemble Techniques—ProQuest. (s. f.). Recuperado 6 de septiembre de 2023, de https://www.proquest.com/openview/afe7ca89f1656bc6daff1d157e23ea25/1?pq-origsite=gscholar&cbl=5444811

Anomaly-based Network Intrusion Detection using Ensemble Machine Learning Approach—ProQuest. (s. f.). Recuperado 6 de septiembre de 2023, de https://www.proquest.com/openview/d9d72dd1b72f456e91148e9657176137/1?pq-origsite=gscholar&cbl=5444811

BCT-CS: Blockchain Technology Applications for Cyber Defense and Cybersecurity: A Survey and Solutions - ProQuest. (s. f.). Recuperado 6 de septiembre de 2023, de https://www.proquest.com/openview/421f66c9054aaffb1ba624e83c2e3757/1?pq-origsite=gscholar&cbl=5444811

COVID-19 malicious domain names classification—ScienceDirect. (s. f.). Recuperado 6 de septiembre de 2023, de https://www.sciencedirect.com/science/article/pii/S0957417422008715

Gawande, R., & Badotra, S. (2022). Deep-Learning Approach for Efficient Eye-blink Detection with Hybrid Optimization Concept. International Journal of Advanced Computer Science and Applications, 13(6). https://doi.org/10.14569/IJACSA.2022.0130693

Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). Machine Learning and Deep Learning Approaches for CyberSecurity: A Review. IEEE Access, 10, 19572-19585. https://doi.org/10.1109/ACCESS.2022.3151248

Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing Detection System Through Hybrid Machine Learning Based on URL. IEEE Access, 11, 36805-36822. https://doi.org/10.1109/ACCESS.2023.3252366

Khan, F., Ncube, C., Ramasamy, L. K., Kadry, S., & Nam, Y. (2020). A Digital DNA Sequencing Engine for Ransomware Detection Using Machine Learning. IEEE Access, 8, 119710-119719. https://doi.org/10.1109/ACCESS.2020.3003785

Larriva-Novo, X. A., Vega-Barbas, M., Villagrá, V. A., & Sanz Rodrigo, M. (2020). Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies. IEEE Access, 8, 9005-9014. https://doi.org/10.1109/ACCESS.2019.2963407

Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. M. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. IEEE Access, 6, 12103-12117. https://doi.org/10.1109/ACCESS.2018.2805680

Luna-López, M., Hernández-Lozano, M., Aldana-Franco, R., Alvarez Sanchez, E., Leyva-Retureta, J., Ricaño-Herrera, F., & Aldana-Franco, F. (2021). Sistema inteligente de monitoreo para condiciones ambientales en Industria 4.0. Científica, 25, 1-10. https://doi.org/10.46842//ipn.cien.v25n2a07

Mahfouz, A., Abuhussein, A., Alsubaei, F., & Shiva, S. (2022). Toward A Holistic, Efficient, Stacking Ensemble Intrusion Detection System using a Real Cloud-

based Dataset. International Journal of Advanced Computer Science and Applications, 13, 2022. https://doi.org/10.14569/IJACSA.2022.01309110

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M.-S., & Zeineddine, H. (2019). An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection. IEEE Access, 7, 93010-93022. https://doi.org/10.1109/ACCESS.2019.2927266

Massaro, A., Gargaro, M., Dipierro, G., Galiano, A. M., & Buonopane, S. (2020). Prototype Cross Platform Oriented on Cybersecurity, Virtual Connectivity, Big Data and Artificial Intelligence Control. IEEE Access, 8, 197939-197954. https://doi.org/10.1109/ACCESS.2020.3034399

Ordoñez-Tumbo, S., Márceles-Villalba, K., Amador-Donado, S., Ordoñez-Tumbo, S., Márceles-Villalba, K., & Amador-Donado, S. (2022). An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT. Ingeniería y Competitividad, 24(2). https://doi.org/10.25100/iyc.v24i2.11762

Otoom, M. M., Sattar, K. N. A., & Al Sadig, M. (2023). Ensemble Model for Network Intrusion Detection System Based on Bagging Using J48. Advances in Science and Technology. Research Journal, Vol. 17(no 2). https://doi.org/10.12913/22998624/161820

Prabha, P. S., & Kumar, S. M. (2022). A Novel Cyber-Attack Leads Prediction System using Cascaded R2CNN Model. International Journal of Advanced Computer Science and Applications, 13(2). https://doi.org/10.14569/IJACSA.2022.0130260

Predicting Malicious Software in IoT Environment Based on Machine Learning and Data Mining Techniques—ProQuest. (s. f.). Recuperado 6 de septiembre de 2023, de https://www.proquest.com/openview/ad34f3c57aa402f75d6047227dbce013/1?pq-origsite=gscholar&cbl=5444811

Rizvi, S., Scanlon, M., Mcgibney, J., & Sheppard, J. (2022). Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions. IEEE Access, 10, 110362-110384. https://doi.org/10.1109/ACCESS.2022.3214506

Sun, B., Ban, T., Han, C., Takahashi, T., Yoshioka, K., Takeuchi, J., Sarrafzadeh, A., Qiu, M., & Inoue, D. (2021). Leveraging Machine Learning Techniques to Identify Deceptive Decoy Documents Associated with Targeted Email Attacks. IEEE Access, 9, 87962-87971. https://doi.org/10.1109/ACCESS.2021.3082000

Wan Ali, W. N. H., Mohd, M., Fauzi, F., Shirai, K., & Noor, M. (2021). IMPLEMENTATION OF HYPERPARAMETER OPTIMISATION AND OVER-SAMPLING IN DETECTING CYBERBULLYING USING MACHINE LEARNING APPROACH. Malaysian Journal of Computer Science, 78-100. https://doi.org/10.22452/mjcs.sp2021no2.6

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access, 8, 146598-146612. https://doi.org/10.1109/ACCESS.2020.3013145

Zhang, S., Xie, X., & Xu, Y. (2020). A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity. IEEE Access, 8, 128250-128263.