ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.723

Machine Learning in Cybersecurity: Systematic Literature Review

Martin Eduardo Valdiviezo Salazar, estudiante de Ingeniería de Sistemas e Informática[1], Fisher Yeferson Huillca Rojas, estudiante de Ingeniería de Sistemas e Informática[2], and Segundo Felipe Alarcón Vázquez, Doctor[3]
[1,2,3] *Universidad Tecnológica del Perú (UTP), Perú U19308755@utp.edu.pe, U19305136@utp.edu.pe, C23460@utp.edu.pe*

Abstract*– Technological advancement has created an urgent demand to strengthen cybersecurity, facing incidents such as Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks. Thus, this systematic review aims to investigate current technologies in cybersecurity, to strengthen digital security and provide key information on the latest trends, contributing to the continuous adaptation of cybersecurity strategies. The methodology, based on the PICO strategy, structures the search in the Scopus and IEEE databases, selecting 21 publications out of a total of 308. The results highlight the complexity of cybersecurity and the variability in the effectiveness of machine learning algorithms, underscoring the importance of careful tool selection. In addition, it is observed that, on average, Decision Tree algorithms achieved 99.59% accuracy for DOS attacks, with a crucial role in defending against cyber threats. The conclusion highlights the critical need for adaptable strategies supported by efficiencies ranging from 41% to 99%, suggesting exploring hybrid approaches and emerging challenges to continuously strengthen cybersecurity. In addition, a 99.6% detection rate underscores the importance of choosing tools carefully, with 32% on false positives and 16% on metrics such as accuracy and recall, emphasizing the need for anticipation and flexibility for effective cybersecurity.

Keywords*-- Network security, Machine learning algorithms, Data Security, Learning Systems.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Machine Learning en Ciberseguridad: Revisión Sistemática de Literatura

Martin Eduardo Valdiviezo Salazar, estudiante de Ingeniería de Sistemas e Informática[1], Fisher Yeferson Huillca Rojas, estudiante de Ingeniería de Sistemas e Informática[2], y Segundo Felipe Alarcón Vázquez, Doctor[3]
[1,2,3] *Universidad Tecnológica del Perú (UTP), Perú U19308755@utp.edu.pe, U19305136@utp.edu.pe, C23460@utp.edu.pe*

Resumen– ***El avance tecnológico ha creado una urgente demanda de reforzar la ciberseguridad, enfrentando incidentes como ataques de Denegación de Servicio (DOS) y Denegación de Servicio Distribuido (DDOS). Es así que esta revisión sistemática tiene como objetivo investigar las tecnologías actuales en ciberseguridad, para fortalecer la seguridad digital y proporcionar información clave sobre las últimas tendencias, contribuyendo a la adaptación continua de estrategias de ciberseguridad. La metodología, basada en la estrategia PICO, estructura la búsqueda en las bases de datos Scopus e IEEE, seleccionando 21 publicaciones de un total de 308. Los resultados destacan la complejidad de la seguridad cibernética y la variabilidad en la efectividad de los algoritmos de machine learning, subrayando la importancia de la cuidadosa selección de herramientas. Además, se observa que, en promedio, los algoritmos Decision Tree alcanzaron una precisión del 99.59% para ataques DOS, con un papel crucial en la defensa contra amenazas cibernéticas. La conclusión destaca la necesidad crítica de estrategias adaptables respaldadas por eficiencias que oscilan entre el 41% y el 99%, sugiriendo explorar enfoques híbridos y desafíos emergentes para fortalecer continuamente la ciberseguridad. Además, una tasa de detección del 99.6% subraya la importancia de elegir herramientas cuidadosamente, con un 32% en falsos positivos y un 16% en métricas como precisión y recall, enfatizando la necesidad de anticipación y flexibilidad para una ciberseguridad efectiva.***

Palabras clave-- ***Network security, Machine learning algorithms, Data Security, Learning Systems.***

I. Introducción

La evolución acelerada de la tecnología ha generado una imperiosa necesidad de fortalecer la seguridad cibernética [1]. Las debilidades en las capas del modelo OSI y en las redes han propiciado un aumento significativo de incidentes de seguridad, como los ataques de Denegación de Servicio (DOS) y Denegación de Servicio Distribuido (DDOS) [2]. Este panorama se ve exacerbado por la expansión desenfrenada de dispositivos de Internet de las Cosas (IoT) conectados sin las medidas de seguridad adecuadas, lo que expone la información a intrusiones y ataques de individuos con intenciones maliciosas [3] [4].

En el ámbito interdisciplinario, el surgimiento de disciplinas como el Machine Learning dentro de la inteligencia artificial han introducido nuevas dimensiones en la seguridad de la información [5]. Aunque la inteligencia artificial puede fortalecer la seguridad, su potencial malicioso plantea desafíos cruciales [6]. La comprensión sólida de las capacidades y restricciones de la inteligencia artificial resulta esencial para implementar estrategias de seguridad efectivas [7].

La relevancia de la inteligencia artificial en ciberseguridad es innegable, desempeñando un papel fundamental en la detección y prevención de amenazas cibernéticas [1], [3]. Sin embargo, la opacidad de los modelos de IA ha suscitado desafíos significativos al dificultar la comprensión humana, lo que constituye la principal motivación de esta investigación [2], [4].

Por lo tanto, el objetivo de este documento se centra en realizar una investigación exhaustiva sobre la situación actual de las tecnologías empleadas en el campo de la ciberseguridad, para el fortalecimiento de esta y hacer frente a los problemas que puedan surgir a consecuencia del desarrollo de nuevas tecnologías, haciéndolas objeto de una RSL cuidadosamente implementada sobre el tema. Contribuyendo a mantener informados a profesionales y organizaciones sobre las últimas tendencias en seguridad digital [3-4], por la presente necesidad ineludible de adaptar continuamente las estrategias de ciberseguridad [1-2].

En tal sentido, este documento sigue una estructura clara y coherente: En la sección 2, Metodología, proporciona detalles sobre el enfoque y métodos utilizados. La sección 3, Resultados, presenta de manera organizada los hallazgos derivados del análisis de la literatura. La sección 4, Discusiones, evalúa críticamente fuentes y tecnologías, ofreciendo una visión general y criterios de interpretación. Finalmente, la sección 5, Conclusiones, sintetiza los principales hallazgos y limitaciones, apuntando hacia futuras direcciones de investigación.

II. Metodología de la Investigación

En este apartado se detallarán los pasos realizados para la búsqueda de publicaciones donde se apliquen algoritmos de machine learning que ayuden a fortalecer la ciberseguridad. Como primer paso, se elabora la pregunta orientadora utilizando la estrategia PICO:

¿Cómo pueden los ataques cibernéticos desafiar los enfoques de seguridad tradicionales y qué papel juega el Machine learning en el fortalecimiento de la ciberseguridad para abordar la vulnerabilidad cibernética?

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Una vez planteada la pregunta orientadora, se procede a examinar cada uno de sus componentes; el problema se enfoca en la vulnerabilidad cibernética, la intervención está determinada por los activos de las organizaciones que son

vulnerables a ataques cibernéticos, la comparación se encuentra determinada en los enfoques de seguridad tradicionales y, por último, los resultados están orientados al fortalecimiento de la ciberseguridad con Machine learning.

TABLA I
COMPONENTES DE LA PREGUNTA PICO

Problema/Población (P)	Vulnerabilidad cibernética
Intervención (I)	Activos vulnerables a ataques cibernéticos
Comparación (C)	Enfoques de seguridad tradicionales
Resultados (O)	El fortalecimiento de la ciberseguridad con Machine learning

Como segundo paso, se identifican las palabras clave a partir de cada componente de la estrategia PICO, como se muestra a continuación.

TABLA II
PALABRAS CLAVE SELECCIONADAS EN BASE A LA METODOLOGÍA PICO

P	I	C	O
Data systems	Computers	Network security	Machine learning algorithms
Data Center	Information	Data Security	Learning Systems

Como tercer paso, se formulan las ecuaciones de búsqueda correspondientes a cada componente de la estrategia PICO con el objetivo de localizar la literatura relevante relacionada con el tema de investigación. Estas ecuaciones de búsqueda serán introducidas en los motores de búsqueda de bases de datos científicas como Scopus y IEEE, seleccionados debido a la calidad de los estudios científicos que contienen y la cantidad de investigaciones que se encuentran relacionadas con el tema de esta revisión. Por lo cual la primera búsqueda fue realizada el 19/09/2023 en la base de datos de Scopus, y se obtuvo un total de 128 documentos, utilizando la siguiente ecuación:

(TITLE-ABS-KEY ("Data centers" OR "Data systems") AND TITLE-ABS-KEY ("Computers" OR "Information") AND TITLE-ABS-KEY ("Network security" OR "data security") AND TITLE-ABS-KEY ("Machine learning algorithms" OR "Learning Systems" OR "Detection algorithms" OR "Cryptography"))

Por otro lado, la segunda búsqueda se realizó el 26/09/2023 en la base de datos de IEEE, obteniendo un total de 180 documentos, donde se utilizó la siguiente ecuación:

("All Metadata":Data centers OR "All Metadata":Data systems) AND ("All Metadata":Computers OR "All Metadata":Information) AND ("All Metadata":Network security OR "All Metadata":data security) AND ("All

Metadata":Machine learning algorithms OR "All Metadata":Learning Systems) AND ("All Metadata":Detection algorithms OR "All Metadata":Cryptography)

En resumen, se obtuvo un total de 308 publicaciones elegibles pertinentes al tema de investigación.

A. Criterios de Inclusión y Exclusión

Con el propósito exclusivo de mejorar los procesos de selección y filtrado de los artículos científicos que serán considerados en este estudio, se procede a la elaboración de los criterios de inclusión y exclusión.

Los criterios de inclusión se establecen de manera detallada, delineando las características esenciales que deben cumplir los estudios para ser considerados pertinentes y relevantes. Por otro lado, los criterios de exclusión son desarrollados para descartar aquellos artículos que no satisfacen los requisitos de este estudio.

TABLA III
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterio de Inclusión	Justificación
CI 1: Los estudios deben abordar temas de algoritmos de Machine learning, enfoques de seguridad tradicionales y vulnerabilidades cibernéticas.	Las publicaciones que se utilizarán deben estar alineadas pertinentemente con el tema y la pregunta de investigación.
CI 2: Los estudios deben aplicar alguna técnica de Machine learning.	En las publicaciones se debe incluir el uso de una herramienta de Machine learning.
CI 3: Los estudios deben incluir resultados estadísticos aplicando técnicas de prevención.	Las publicaciones deben contener resultados que demuestren la eficacia de los modelos propuestos.
CI 4: Los estudios deben haber sido realizados en entornos reales.	Es esencial evaluar su eficacia en situaciones reales.
Criterio de Exclusión	**Justificación**
CE 1: Publicaciones que estén fuera del rango de fechas relevantes (2018)	Trabajar con publicaciones actualizadas
CE 2: Estudios en idiomas no accesibles o traducibles por el equipo de investigación.	Trabajar con fuentes de entendimiento directo sin utilizar herramientas de traducción que pueden ser imprecisas.
CE 3: Publicaciones con el título no relacionado al tema.	Identificar estudios que no estén relacionados con el tema de investigación
CE 4: Publicaciones duplicadas o redundantes.	Descartar publicaciones repetidas que se encuentran en ambas bases de datos.

B. Resultados de la Búsqueda

En primera instancia, las búsquedas se llevaron a cabo en las bases de datos Scopus e IEEE para lo cual se utilizaron las ecuaciones de búsqueda previamente especificadas. Estas búsquedas arrojaron un total de 128 y 180 estudios, respectivamente, lo que sumó un conjunto inicial de 308 publicaciones.

Asimismo, se aplicaron los criterios de exclusión (CE). Según estos criterios, se procedió con la eliminación de duplicados (CE 4), lo que resultó en la exclusión de aproximadamente 28 documentos, reduciendo así el número de publicaciones elegibles a 280. De estos documentos, 26 artículos se encontraban alejadas del rango de fechas relevantes (CE 1), 17 estudios estaban en idiomas no accesibles o traducibles (CE 2), y 209 no estaban directamente relacionados con el tema de interés (CE 3). Y se descartaron documentos ya que utilizaban componentes especializados, lo cual se desviaba de nuestro tema central. Como resultado de la aplicación de estos criterios, se excluyeron un total de 259 fuentes, lo que condujo a la selección final de 21 estudios que cumplieron con los requisitos establecidos.

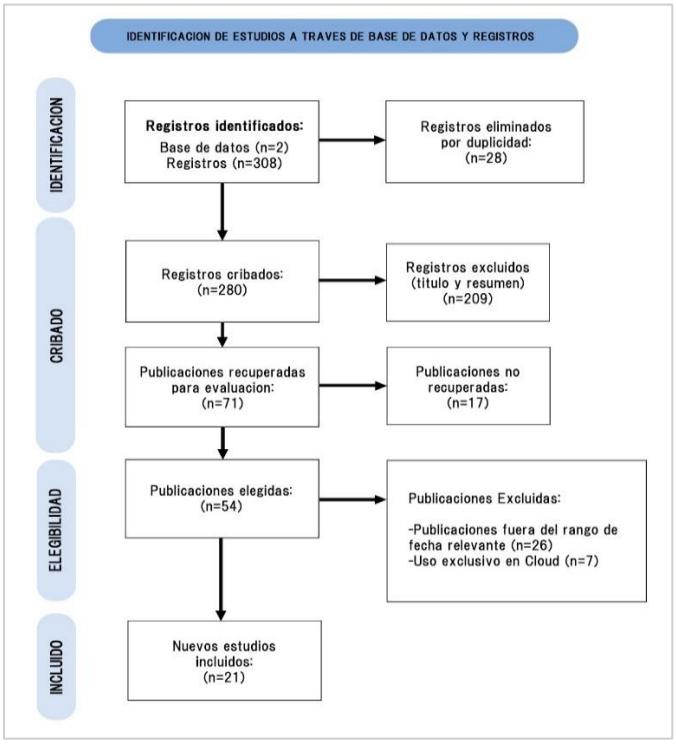

Fig 1 Diagrama PRISMA

III. RESULTADOS

RQ1: ¿Cómo se ha definido la seguridad cibernética?

La seguridad cibernética se presenta como un campo multidimensional crítico para salvaguardar la integridad y operatividad de los sistemas informáticos [5]. Este concepto abarca un conjunto de mecanismos y técnicas diseñadas para proteger sistemas de big data contra amenazas y ataques cibernéticos [5-6]. Ampliando este enfoque, se destaca su papel en la protección integral de sistemas informáticos y redes contra diversas amenazas cibernéticas [1-2]. Desde la protección de información hasta la manera de contrarrestar los ciberataques, estas definiciones reflejan la diversidad y complejidad del ámbito de la seguridad cibernética.

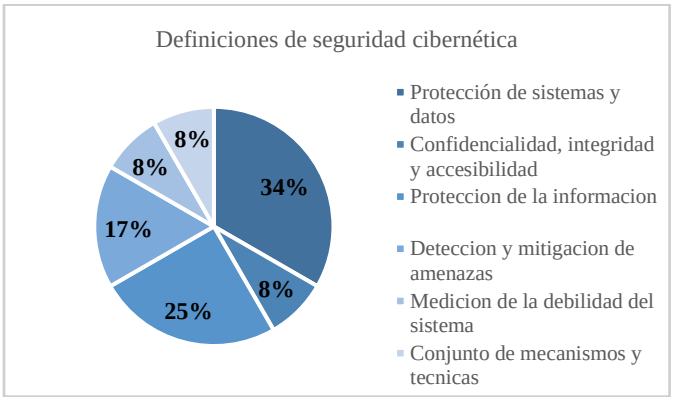

Fig 2 Definiciones de seguridad cibernética

RQ2: ¿Qué tipos de ataques cibernéticos fueron abordados en el estudio?

La complejidad y diversidad de amenazas cibernéticas abordadas en los estudios revisados revelan un panorama de riesgos significativo. Se identifican ataques internos, inyecciones de código java y ataques DOS [5], mientras que se detallan ataques por la puerta de atrás, exploit attacks y ataques de código de shell [6]. Otros estudios categorizan una amplia gama de tipos, incluyendo XSS, Clickjacking, DOS, U2R, R2L y Probe [7]. Esta diversidad incluye malware, phishing y ataques en sistemas SCADA, ofreciendo una visión integral de los riesgos en la seguridad cibernética, desde amenazas comunes hasta aquellas específicas de entornos críticos.

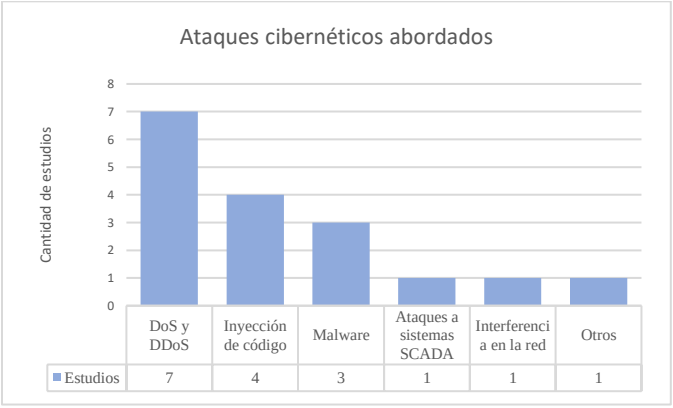

Fig 3 Análisis de ataques cibernéticos abordados

RQ3: ¿Qué enfoques de seguridad tradicionales quedan vulnerables ante nuevas tecnologías?

La preocupación sobre la vulnerabilidad de enfoques tradicionales de seguridad ante el avance tecnológico y la

sofisticación de las amenazas es recurrente en los estudios revisados. Se expone la vulnerabilidad de sistemas Hadoop y ACL, subrayando la necesidad de adaptarse a las complejidades de sistemas de big data [5]. Se destaca la insuficiencia de sistemas de detección de intrusiones ante tecnologías emergentes como IoT [3]. También se menciona la exposición en escenarios del internet de las cosas y redes neuronales [8]. Estas adaptaciones son esenciales para abordar las vulnerabilidades inherentes a entornos en constante cambio y garantizar la eficacia continua de las estrategias de seguridad.

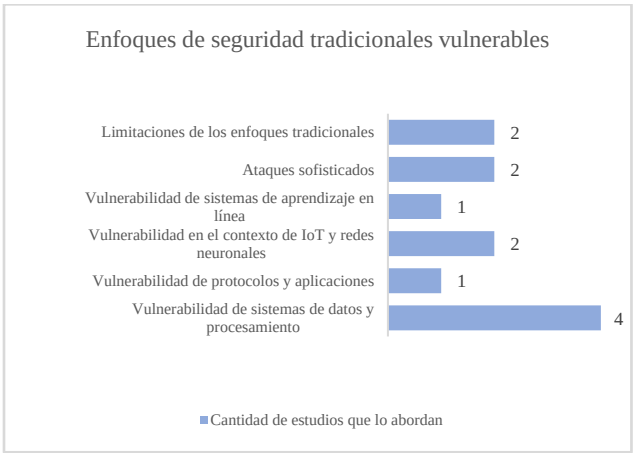

Fig 4 Enfoques vulnerables

RQ4: ¿Qué nivel de eficacia se ha obtenido al aplicar algoritmos de machine learning para la detección de amenazas cibernéticas?

La efectividad de los algoritmos de machine learning en la detección de amenazas cibernéticas se revela como un aspecto crítico pero variado en los estudios revisados. Los algoritmos Decision Tree alcanzan una precisión destacada del 99.59% para ataques DOS [6]. Jiang et al. [7] logran una tasa de detección del 99.6% con bajos falsos positivos. Paliwal y colaboradores [1] reportan una precisión del 99.7% mediante SVM. Sin embargo, se señala una eficacia inferior al 3.28% bajo ciertos contextos, resaltando la importancia de seleccionar y evaluar cuidadosamente los algoritmos de machine learning [9]. Considerando las particularidades de los conjuntos de datos y los tipos de amenazas, se optimiza la efectividad de las soluciones de seguridad cibernética.

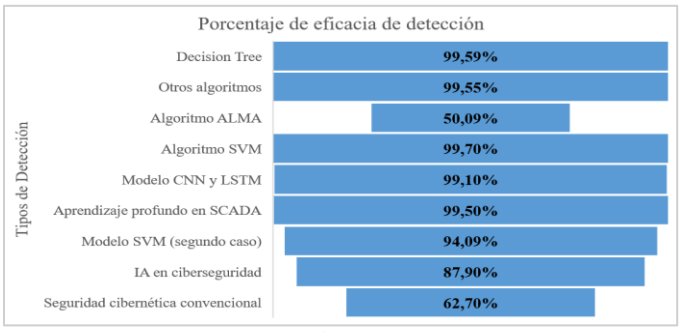

Fig 5 Enfoques vulnerables

RQ5: ¿Qué modelo de machine learning fue utilizado en el estudio?

En el contexto de la investigación, una variedad de modelos de machine learning fue empleada, abarcando desde métodos clásicos como Decision tree, Naive-bayes, glm-classification, glm-regression [5], hasta enfoques más avanzados como k-Nearest Neighbor (KNN), support vector machine (SVM) [10], y Markov decision process [11]. Además, se exploraron modelos basados en redes neuronales profundas, reconocidos por su capacidad para extraer patrones complejos [2], junto con otras técnicas, tales como online learning, Perceptron, y Random Forest [12].

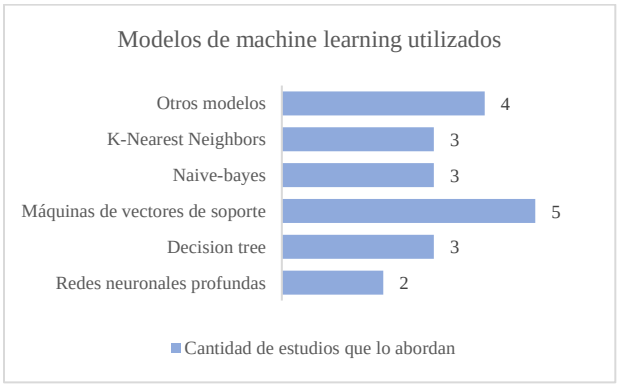

Fig 6 Modelos de Machine Learning utilizados

RQ6: ¿Qué métricas se utilizaron para evaluar la efectividad de las herramientas de machine learning en ciberseguridad?

La evaluación de las herramientas de machine learning en ciberseguridad se basó en diversas métricas. Entre ellas, se consideraron el tiempo de ejecución del ataque, precisión, tasa de detección de amenazas, tasa de falsas alarmas y especificidad [5]. Asimismo, se evaluó la pérdida de carga eléctrica en dispositivos [11], y se emplearon métricas como tasa de error acumulada, tasa positiva verdadera, área bajo la curva ROC (AUC) [2], abordando así distintos aspectos de la efectividad de estas herramientas.

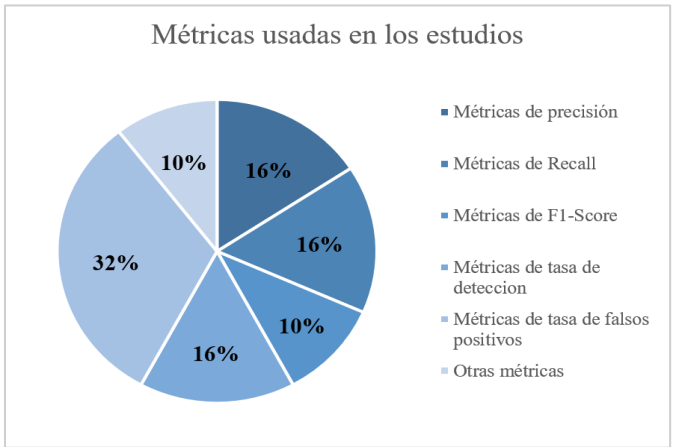

Fig7 Métricas para definir la efectividad de los algoritmos

RQ7: ¿Qué métodos fueron discutidos en el estudio?

En el transcurso del estudio, se discutieron diversos métodos, desde los modelos de ataque y defensa [1], [2], [5], [6], [13], [14], [17], [19], [20], [21], diseñado para abordar amenazas específicas, hasta los de aprendizaje de máquina y métodos de mejora [7], [9], [11], [16], una metodología para identificación automática de vulnerabilidades [11]. La investigación también consideró enfoques de tecnología de aprendizaje profundo [1],[17],[19] y propuso métodos basados en minería de datos, aprovechando múltiples canales de procesamiento [4]. Adicionalmente, se exploraron enfoques de aprendizaje centralizado y federado [8], el cual se enfocó especialmente en entornos como el Internet de las Cosas (IoT).

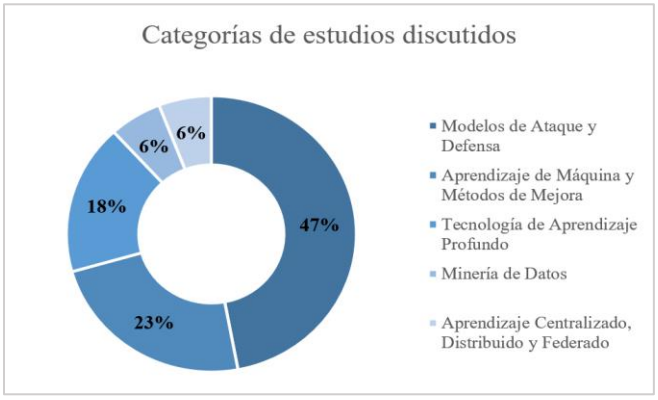

Fig 8 Métodos discutidos

RQ8: ¿Qué tipos de vulnerabilidades fueron tratadas en el estudio?

En el marco del estudio, se abordaron diversas vulnerabilidades en ciberseguridad. Estas incluyeron desde vulnerabilidades en protocolos específicos como TCP/IP y SSH [5], hasta desafíos relacionados con redes de sistemas Big Data [10]. Además, se trató la problemática de ciberataques, errores humanos y desastres [11]. El estudio también se centró en vulnerabilidades asociadas a protocolos TCP/IP y servicios web [2], así como amenazas más específicas como ataques DDoS, inyecciones SQL, administración de sesiones y configuraciones de seguridad [12].

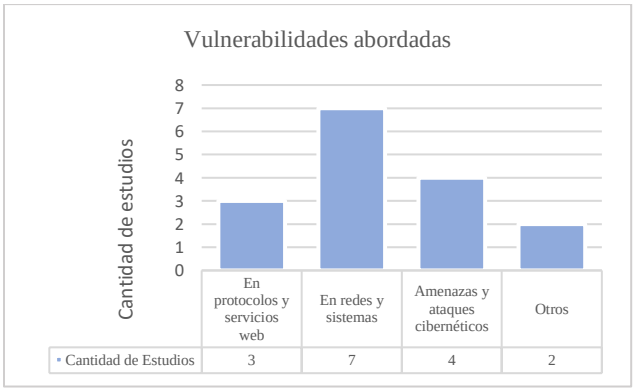

Fig 9 Tipos de vulnerabilidades

IV. Discusión

Explorando diversas perspectivas, Aditham y Ranganathan [1] conceptualizan la seguridad cibernética como un conjunto de mecanismos y técnicas (8% de los estudios) [5], resaltando la complejidad inherente al campo. En contraste, Alhabshy et al. [2] enfatizan la necesidad de mejorar la detección de amenazas (17% de los estudios) [6], subrayando la constante evolución de las tácticas de los atacantes. Kang et al. [3], al introducir la noción de medición de la debilidad del sistema frente a eventos en cascada (8% de los estudios) [7], destacan la importancia de evaluar la resistencia ante posibles ataques en cadena. Estas interpretaciones se entrelazan con las propuestas de Manuel et al. [4], quienes consideran la seguridad cibernética como un conjunto de soluciones para contrarrestar ciberataques (25% de los estudios) [8].

Por otro lado, las investigaciones de Aditham y Ranganathan [1] identifican ataques internos mediante scripts, ataques DOS e inyecciones de código java, mientras que Alhabshy et al. [2] profundizan en ataques por la puerta de atrás, exploit attacks y ataques de código de shell. La categorización amplia de Jiang et al. [5] proporciona una visión comprehensiva de las amenazas, desde las comunes hasta las específicas de entornos críticos, abarcando desde XSS y Clickjacking hasta DoS, U2R, R2L y Probe. En cuanto a la clasificación, se evidencia la relevancia de ataques de denegación de servicio (DoS) y distribuidos (DDoS) en 7 estudios [1], [2], [7], [12], [13], [14], [15], [18]; junto con la persistencia de ataques de inyección de código en 4 estudios [3], [6], [9], [11]. La atención a amenazas específicas, como el malware y los ataques al sistema SCADA, resalta la necesidad de estrategias de protección adaptativas. Además, uno de los estudios aborda amenazas diversas, desde la intercepción de datos hasta la penetración de usuarios y virus, subrayando la complejidad del paisaje de seguridad cibernética [8].

Asimismo, la variabilidad en la efectividad de los algoritmos de machine learning, como se evidencia en los estudios revisados, subraya la importancia de una selección y evaluación meticulosas de estos algoritmos para la detección de amenazas cibernéticas [6], [7], [9]. Aunque el Decision Tree y SVM exhiben altas precisiones de hasta el 99.7% para ciertos tipos de ataques, como los ataques DOS [1], [6], es crucial reconocer las condiciones bajo las cuales estos resultados pueden no ser replicables. Por ejemplo, en un estudio se señala una eficacia significativamente inferior al 3.28% bajo ciertos contextos [9], lo cual puede ser indicativo de limitaciones en el entrenamiento del modelo o en la calidad de los datos utilizados. Es así que este análisis refuerza la necesidad de considerar factores adicionales como el tamaño del dataset, la interpretación de los modelos, y los recursos computacionales disponibles [20]. Además, los porcentajes de eficacia varían, con 99.55% para otros métodos y 50.09% para ALMA [5]. SVM [1], modelo CNN y LSTM [11], y aprendizaje profundo en SCADA [19] exhiben notables eficacias de 99.70%, 99.10%, y 99.50%, respectivamente. También, se observa que el segundo método de detección del modelo SVM obtiene el

94.09% [3], contrastando con el 87.90% para la inteligencia artificial en ciberseguridad [17], y la seguridad cibernética convencional alcanza el 62.70% [16].

V. Conclusiones

Esta revisión sistemática ha explorado exhaustivamente las tecnologías de ciberseguridad, resaltando la necesidad crítica de estrategias adaptables respaldadas por eficiencias que oscilan entre el 41% y el 99%. La creciente interconexión de dispositivos y sistemas ha revelado una vulnerabilidad significativa ante el rápido desarrollo tecnológico, evidenciada claramente en la insuficiencia de las estrategias actuales frente al Internet de las cosas (IoT), lo cual señala una urgencia de evolución constante en las estrategias de ciberseguridad para mantenerse a la par con las cambiantes amenazas cibernéticas.

En el ámbito de los algoritmos de machine learning, la diversidad en las tasas de detección, alcanzando un impresionante 99.6%, resalta la importancia crucial de una cuidadosa selección de herramientas. A pesar de las métricas diversas, con un enfoque del 32% en la tasa de falsos positivos y un 16% considerando precisión, recall y la tasa de detección, se evidencia la complejidad del panorama cibernético. La variedad de métodos discutidos subraya la necesidad apremiante de adaptarse a esta dinámica, donde la anticipación y la flexibilidad en la elección de herramientas se convierten en pilares fundamentales para una ciberseguridad efectiva.

Reconociendo las limitaciones, como la rápida evolución del entorno cibernético y posibles influencias de la calidad de datos, se sugiere para futuros trabajos explorar enfoques híbridos que integren diversas técnicas de protección, adaptándose a la dinámica del panorama cibernético. Además, se recomienda investigar desafíos emergentes, como la convergencia de inteligencia artificial y ciberseguridad, y enfocarse en el desarrollo de técnicas avanzadas para la detección y prevención de amenazas, con énfasis en la eficacia y eficiencia. Estas áreas de investigación pueden contribuir significativamente al fortalecimiento continuo de la ciberseguridad.

Referencias

[1] S. Paliwal, V. Bharti, y A. K. Mishra, "Machine learning combating DOS and DDOS attacks", Int J Bus Inf Syst, vol. 40, núm. 2, pp. 177–191, 2022, doi: 10.1504/IJBIS.2022.123638.

[2] F. Charmet et al., "Explainable artificial intelligence for cybersecurity: a literature survey", Annales des Telecommunications/Annals of Telecommunications, vol. 77, núm. 11–12, pp. 789–812, dic. 2022, doi: 10.1007/S12243-022-00926-7/TABLES/3.

[3] D. K. Sharma, J. Mishra, A. Singh, R. Govil, G. Srivastava, y J. C. W. Lin, "Explainable Artificial Intelligence for Cybersecurity", Computers and Electrical Engineering, vol. 103, p. Article 108356, oct. 2022, doi: 10.1016/j.compeleceng.2022.108356.

[4] J. Manuel, R. Cordeiro, y C. Silva, "Between Data Mining and Predictive Analytics Techniques to Cybersecurity Protection on eLearning Environments", Advances in Intelligent Systems and Computing, vol. 662, pp. 185–194, 2018, doi: 10.1007/978-3-319-67621-0_17.

[5] D. Aiyanyo, H. Samuel, y H. Lim, "A systematic review of defensive and offensive cybersecurity with machine learning", Applied Sciences (Switzerland), vol. 10, núm. 17, p. Article 5811, sep. 2020, doi: 10.3390/app10175811.

[6] A. Alhabshy, B. I. Hameed, y K. A. Eldahshan, "An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers", IEEE Access, vol. 10, pp. 52724–52743, 2022, doi: 10.1109/ACCESS.2022.3174482).

[7] F. Jiang et al., "Deep Learning Based Multi-Channel Intelligent Attack Detection for Data Security", IEEE Transactions on Sustainable Computing, vol. 5, núm. 2, p. 8259310, abr. 2020, doi: 10.1109/TSUSC.2018.2793284.

[8] E. M. Campos et al., "Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges", Computer Networks, vol. 203, p. Article 108661, feb. 2022, doi: 10.1016/j.comnet.2021.108661.

[9] S. Aditham y N. Ranganathan, "A System Architecture for the Detection of Insider Attacks in Big Data Systems", IEEE Trans Dependable Secure Comput, vol. 15, núm. 6, pp. 974–987, nov. 2018, doi: 10.1109/TDSC.2017.2768533).

[10] H. Cam, "Model-Guided Infection Prediction and Active Defense Using Context-Specific Cybersecurity Observations", Proceedings - IEEE Military Communications Conference MILCOM, vol. 2019, p. Article 9020980, nov. 2019, doi: 10.1109/MILCOM47813.2019.9020980.

[11] Y. Xin et al., "Machine learning and Deep Learning Methods for Cybersecurity", IEEE Access, vol. 6, pp. 35365–35381, may 2018, doi: 10.1109/ACCESS.2018.2836950.

[12] Alshehri, N. Khan, A. Alowayr, y M. Y. Alghamdi, "Cyberattack Detection Framework Using Machine learning and User Behavior Analytics", Computer Systems Science and Engineering, vol. 44, núm. 2, pp. 1679–1689, 2023, doi: 10.32604/csse.2023.026526.

[13] Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, y S. R. Gulliver, "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature", IEEE Access, vol. 8, p. 9152956, 2020, doi: 10.1109/ACCESS.2020.3013145.

[14] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, y M. Pasha, "Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system", Neural Comput Appl, vol. 34, núm. 1, pp. 493–514, ene. 2022, doi: 10.1007/s00521-021-06400-0.

[15] J. Martínez Torres, C. Iglesias Comesaña, y P. J. García-Nieto, "Review: machine learning techniques applied to cybersecurity", International Journal of Machine learning and Cybernetics, vol. 10, núm. 10, pp. 2823–2836, oct. 2019, doi: 10.1007/s13042-018-00906-1.

[16] R. Kaur, D. Gabrijelčič, y T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions", Information Fusion, vol. 97, p. Article 101804, sep. 2023, doi: 10.1016/j.inffus.2023.101804.

[17] Q. Liu y T. Zhang, "Deep learning technology of computer network security detection based on artificial intelligence", Computers and Electrical Engineering, vol. 110, p. Article 108813, sep. 2023, doi: 10.1016/j.compeleceng.2023.108813.

[18] L. Yaser, H. M. Mousa, y M. Hussein, "Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder", Future Internet, vol. 14, núm. 8, p. Article 240, ago. 2022, doi: 10.3390/fi14080240.

[19] S. Y. Diaba et al., "SCADA securing system using deep learning to prevent cyber infiltration", Neural Networks, vol. 165, pp. 321–332, ago. 2023, doi: 10.1016/j.neunet.2023.05.047.

[20] G. Li et al., "Detecting cyberattacks in industrial control systems using online learning algorithms", Neurocomputing, vol. 364, pp. 338–348, oct. 2019, doi: 10.1016/j.neucom.2019.07.031.

[21] C. Kang et al., "An automatic algorithm of identifying vulnerable spots of internet data center power systems based on reinforcement learning", International Journal of Electrical Power and Energy Systems, vol. 121, p. Article 106145, oct. 2020, doi: 10.1016/j.ijepes.2020.106145.u