ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.368

A Systematic Review on the Evaluation of Advanced Approaches in Cyberattack Detection

Jordan Piero Gonzales Barcayola[1]; Juan Jose Gomez Lizama[2]; Luis Enrique Cuevas Tenorio[3]
[1,2,3] Universidad Tecnológica del Perú, Perú
U19211847@utp.edu.pe, U20216247@utp.edu.pe, C28109@utp.edu.pe

***Abstract*– This article presents a comprehensive study on the detection of cyberattacks on websites, highlighting the increase in threats such as phishing, SQL injection and DDoS attacks, which compromise data security and user trust. Through a methodology aimed at the review and collection of 21 recent studies, methods based on artificial intelligence were evaluated, such as neural networks and behavioral analysis, which surpass traditional approaches, such as firewalls and IDS, in precision and adaptability. The results underline that the most effective strategies are based on adaptive approaches and emerging technologies, integrating dynamic systems capable of responding to contextual changes and advanced analytical tools to mitigate risks. This review contributes to consolidating an updated and detailed overview, identifying knowledge gaps and establishing a solid foundation for the development of innovative and robust solutions that strengthen security in modern web applications.**

***Keywords*-- Cyberattacks, Machine Learning, Artificial Intelligence, Web Applications Security, Neural Networks.**

Una revisión sistemática en la Evaluación de Enfoques Avanzados en la Detección de Ataques Cibernéticos

Jordan Piero Gonzales Barcayola[1]; Juan Jose Gomez Lizama[2]; Luis Enrique Cuevas Tenorio[3]
[1,2,3] Universidad Tecnológica del Perú, Perú.
U19211847@utp.edu.pe, U20216247@utp.edu.pe, C28109@utp.edu.pe

***Resumen*– Este artículo presenta una sistematización de las principales investigaciones sobre la detección de ciberataques en sitios web, destacando el aumento de amenazas como phishing, inyección SQL y ataques DDoS, las cuales comprometen la seguridad de los datos y la confianza de los usuarios. A través de una metodología orientada a la revisión y recolección de 21 estudios recientes, se evaluaron métodos basados en inteligencia artificial, como redes neuronales y análisis conductual, los cuales superan en precisión y adaptabilidad a los enfoques tradicionales, como firewalls e IDS. Los resultados subrayan que las estrategias más efectivas se basan en enfoques adaptativos y tecnologías emergentes, integrando sistemas dinámicos capaces de responder a cambios contextuales y herramientas analíticas avanzadas para mitigar riesgos. Esta revisión contribuye a consolidar un panorama actualizado y detallado, identificando brechas de conocimiento y estableciendo una base sólida para el desarrollo de soluciones innovadoras y robustas que fortalezcan la seguridad en aplicaciones web modernas.**

***Palabras clave:* Ciberataques, Aprendizaje Automático, Inteligencia Artificial, Seguridad en Aplicaciones Web, Redes Neuronales.**

I. Introducción

En la época digital, la seguridad cibernética ha destacado por resguardar la información en línea, sobre todo en plataformas web con cuantiosa información delicada. Diversos estudios han mostrado que el número de ataques cibernéticos ha aumentado considerablemente en los últimos años, afectando tanto a grandes organizaciones como a pequeñas empresas, con consecuencias devastadoras que incluyen pérdida de datos, interrupción de servicios y daños a la reputación de las organizaciones afectadas [1]. Por ejemplo, ataques phishing, la inyección SQL (Lenguaje de Consulta Estructurada), la denegación de servicio (DDoS), entre otras son las más reiterativas por los ciberdelincuentes. Debido a ello, estas amenazas sitúan en peligro grandes cantidades de información empresarial. Asimismo, perjudican al usuario vulnerando la integridad y confidencialidad de la página. Por ello, se indica que la protección de estos recursos se ha convertido en una prioridad crítica para asegurar la integridad y la discreción de la información y mantener la confianza de los usuarios.

El problema central consiste en que los métodos clásicos de seguridad. Por ejemplo, VPN (Red Privada Virtual), los firewalls, cifrado de datos y los sistemas de detección de intrusos (IDS), aunque son prácticos no son suficientes para afrontar las amenazas modernas, particularmente en ataques complejos o novedosos. Por ejemplo, los ataques de phishing han evolucionado al punto de utilizar técnicas de evasión basadas en inteligencia artificial para burlar los sistemas de detección convencionales [2]. Asimismo, la creciente complejidad de la infraestructura web, que incluye servicios en la nube y arquitecturas basadas en contenedores, amplía la superficie de ataque y dificulta la implementación de soluciones de seguridad robustas y escalables [3].

En este ámbito, la detección de ciberataques en sitios web por intermedio de métodos avanzados de aprendizaje automático (ML) y optimización se ha transformado en un espacio de investigación crítica. Investigaciones recientes han explorado enfoques híbridos que combinan características y optimización para mejorar la precisión y eficiencia en la detección de ataques, abordando la necesidad de soluciones más adaptativas y resistentes [4][5]. Sin embargo, la velocidad a la que progresan las técnicas de ataque y las complejidades de las infraestructuras web recientes, resaltan la necesidad de una evaluación continua y el aumento de nuevas tecnologías de detección.

Desarrollar una Revisión Sistemática de Literatura (RSL) en referencia a la identificación de ataques de ciberseguridad en sitios web es de suma importancia para que de esa forma se llegue a consolidar y evaluar los métodos existentes en el campo de investigación. Esta revisión permitirá la identificación de prácticas actuales más efectivas. En un contexto donde se está en constante cambio, es fundamental tener la información de manera extensa y actualizada de los diferentes métodos disponibles para una protección eficaz, con el objetivo de brindar un fundamento firme para el desarrollo de soluciones más robustas y adaptativas en este campo.

Es importante aclarar que este artículo de revisión no tendrá carácter periódico, sino que consistirá en una revisión única destinada a la construcción de conocimiento.

II. METODOLOGÍA

En la Revisión Sistemática de la Literatura se llevó a la práctica la metodología PIOC (Problema, Intervención, Resultados, Contexto) [6] sin metaanálisis. Esta metodología posibilitó proponer la siguiente pregunta de investigación central: ¿Qué tan efectivos son los métodos basados en inteligencia artificial para la detección de ataques cibernéticos en diferentes tipos de sitios web? De la pregunta general se estableció 4 sub preguntas relacionadas con cada componente del PIOC como se muestra en la Tabla I.

TABLA I
TABLA DE LAS PREGUNTAS POR CADA COMPONENTE DEL PIOC

P	**Problema**	*¿Qué tipos de ataques cibernéticos han afectado a los sitios web?*
I	**Intervención**	*¿Qué métodos basados en inteligencia artificial se han aplicado para la detección de ataques cibernéticos en sitios web?*
O	**Resultado**	*¿Qué niveles de eficiencia han mostrado los métodos basados en inteligencia artificial en tasas de detección?*
C	**Contexto**	*¿En qué tipos de sitios web se ha investigado la detección de ataques cibernéticos?*

FUENTE: ELABORACIÓN PROPIA

Se identificó las palabras claves por cada elemento del PIOC como se muestra en la Tabla II.

TABLA II
PALABRAS CLAVES

P	**PROBLEMA**	Ataques Cibernéticos.	Cyberattacks
			Web vulnerabilities
			Website security
			Data breaches
			Threats to web systems
I	**INTERVENCIÓN**	Métodos basados en inteligencia artificial	Artificial Intelligence
			Machine Learning
			Behavioral Analysis
			Neural Networks
			Adaptive Detection
O	**RESULTADOS**	Efectividad de Detección	Detection speed
			False positive
			True positive
			Response time
			Detection rate
C	**CONTEXTO**	Sitios Web	*Websites*
			Web application security
			Social media
			Educational institutions
			Financial website

FUENTE: ELABORACIÓN PROPIA

En relación con las palabras clave se formuló la siguiente ecuación de búsqueda sistemática de literatura. En consecuencia, dio como resultado a la siguiente ecuación de búsqueda (1).

("Cyberattacks" OR "Web vulnerabilities" OR "Website security" OR "Data breaches" OR "Threats to web systems") AND ("Artificial Intelligence" OR "Machine Learning" OR "Behavioral Analysis" OR "Adaptive Detection" OR "Neural Networks") AND (" Detection" OR "Accuracy " OR "Detection speed" OR "False positive" OR "True positive" OR "Response time" OR "Detection rate") AND ("website" OR "websites" OR "Social media" OR "Educational institutions" OR "Financial websites" OR "Web application security")

También, se crearon los criterios de inclusión para la selección de estudios, que se detallan a continuación:

CI 1 Los estudios incluidos deben incluir una variedad de tipos de sitios web.
CI 2 Los estudios deben presentar investigaciones que analicen incidentes de ataques cibernéticos.
CI 3 Los estudios deben enfocarse en la implementación de tecnologías para la detección de ataques.
CI 4 Los estudios deben operar como los sitios web analizados y cómo afecta a la efectividad de las técnicas de detección.

De igual manera, se establecieron los criterios de exclusión de la selección de estudios, que se describen a continuación:

CE 1 Tipo de publicación NO corresponde al artículo.
CE 2 Publicaciones en idiomas diferentes al inglés.
CE 3 Documentos anteriores a 2019.
CE 4 Documentos que no hablen de ataques cibernéticos

De acuerdo a lo anteriormente señalado, los estudios seleccionados fueron evaluados por la herramienta Prisma [7] Por ello, se inició con la fase de identificación donde se encontraron 165 estudios en la base de datos Scopus, donde no se encuentra registros duplicados, ya que no se realizó la búsqueda en otra base de datos, quedaron la misma cantidad de registros 165 antes del cribado. Luego se llevó a cabo la exclusión a partir de la lectura de títulos y resúmenes, dónde 58 estudios se retiraron por no abarcar el tema de investigación, Asimismo, quedaron un total de 103 documentos. Se realizaron las descargas para identificar publicaciones no recuperadas donde 10 estudios no fueron posibles ver su contenido, teniendo un total de 93 documentos.

Por último, se excluyeron 45 documentos identificados como conference paper y conference review, de acuerdo con los criterios planteados. Asimismo, siguiendo el criterio de

exclusión de estudios que son en otro idioma diferente al inglés no se excluyó ningún estudio. Posteriormente, al aplicar criterio de estudios anteriores al 2019, se identificaron 4 estudios diferentes al año mencionado. Por último, se identificaron 23 estudios que no están relacionados con ataques cibernéticos, donde quedaron 21 artículos que serán de utilidad para la realización de una RSL. Como se detalla en la figura 1.

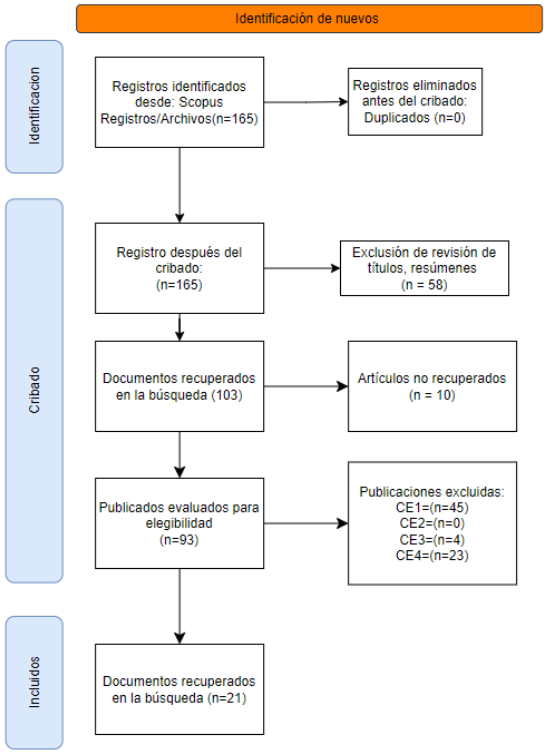

Fig. 1 Esquema de diagrama prisma propuesto.

III. RESULTADOS

En esta sección se describen los reportes obtenidos de todos los 21 artículos revisados en la investigación, representado mediante tablas e ilustraciones que ayudarán a entender los datos recabados, los cuales estos datos se dividen en cualitativos y cuantitativos. Asimismo, la información nos permite dar respuesta a las preguntas planteadas en el estudio.

A. ¿Qué tipos de ataques cibernéticos han afectado a los sitios web?

Los estudios revisados abordan diversos ataques cibernéticos y se centran en el phishing, utilizando URLs y correos electrónicos fraudulentos para suplantar identidades y robar datos sensibles [8], [9]; sin embargo, también se exploran otros ataques como Cross-Site Scripting (XSS) y SQL Injection, que explotan vulnerabilidades en aplicaciones web con la inyección y manipulación de código para ejecutar código malicioso y acceder a bases de datos [10], [11]. Además, se consideran tácticas como el robo de credenciales, la fuerza bruta, y la manipulación de sitios web (Defacement) [12], [13], así como el uso de malware, troyanos, y hardware [14]. Algunos estudios abordan amenazas específicas en redes sociales y aplicaciones web, tales como *spoofing*, scam, y bots maliciosos utilizados para fraude de clics y ataques DDoS [8], [9], como se muestra en la Tabla III. Asimismo, en la figura 1, se muestran los ataques más investigados los ataques basados en la manipulación y el engaño (phishing, *spoofing*, URLs maliciosas), así como aquellos que explotan vulnerabilidades en aplicaciones web (XSS, inyección SQL) y Malwares [15], [16].

TABLA III
FRECUENCIA DE ATAQUES CIBERNÉTICOS INVESTIGADOS

Categoría de Ataque	**Tipos de ataques incluidos**	**Frecuencia Total**
Phishing y Suplantación	Phishing, URLs Maliciosas, Drive-by Download, *Spoofing*, Scam	21
Inyecciones y Manipulación de Código	XSS (Cross-Site Scripting), Inyecciones SQL, Cross-Site Request Forgery (CSRF), Desbordamiento de Búfer	**7**
Malware y Software Malicioso	Malware, Troyanos, Adware	**5**
Interrupción de Servicio	Denial of Service (DoS), DDoS a Nivel de Aplicación	**2**
Acceso y Autenticación	Ingeniería Social en Redes Sociales, Ataques de Fuerza Bruta, Reutilización de Contraseñas, Robo de Credenciales	**4**
Alteración y manipulación de contenido	Defacement, Problemas de configuración de Cookies HTTP, Bots Maliciosos, Spam	**5**

FUENTE: ELABORACIÓN PROPIA

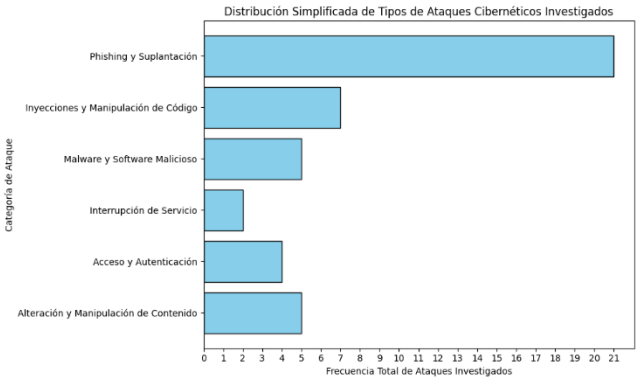

Fig. 2. Frecuencia de ataques cibernéticos investigados

B. ¿Qué métodos basados en inteligencia artificial se han aplicado para la detección de ataques cibernéticos en sitios web?

Los métodos basados en inteligencia artificial aplicados para la detección de ataques cibernéticos en sitios web incluyen una variedad de técnicas de aprendizaje automático y profundo, que destacan por su capacidad de identificar patrones en el tráfico y contenido malicioso. Las redes neuronales convolucionales (CNN) han sido ampliamente utilizadas debido a su habilidad para extraer características de URLs (Localizador Uniforme de Recursos) y clasificarlas con precisión, demostrando tasas de detección elevadas en entornos experimentales [8]. Además, el uso de algoritmos de árboles de decisión y bosque aleatorio (Random Forest) ha sido efectivo en la detección de phishing, particularmente en la identificación de URLs maliciosas a través de la selección de características relevantes [9], [10]. Otros estudios han implementado enfoques de aprendizaje en ensamble, como el *boosting* adaptativo, que combina clasificadores débiles para aumentar la precisión y reducir las tasas de falsos positivos [19]. Técnicas avanzadas como el uso de transformers en combinación con expertos mixtos también se han explorado para el análisis de phishing, aprovechando la capacidad de los modelos profundos para procesar y clasificar grandes volúmenes de datos de sitios web [20]. Por último, enfoques híbridos que integran modelos de redes neuronales con algoritmos tradicionales de aprendizaje automático han mostrado resultados prometedores en términos de eficiencia y efectividad en la clasificación de URLs maliciosas y legítimas [21]. Estos métodos se muestran en la Tabla IV donde los frameworks de redes neuronales fueron los más utilizados, como Keras y Tensor Flow, con una frecuencia de 10 estudios cada uno.

TABLA IV

MÉTODOS DE IA PARA LA DETECCIÓN

Métodos de IA	Frecuencia Total	Principales Herramientas Utilizadas
Redes Neuronales	25	Keras (10), TensorFlow (10), Scikit-Learn (2), Otras (3)
Modelos Basados en Árboles	12	Scikit-Learn (10), Otras (2)
Otros Métodos	21	Scikit-Learn (15), Keras (1), TensorFlow (1), MATLAB (1), Otras (3)

FUENTE: ELABORACIÓN PROPIA

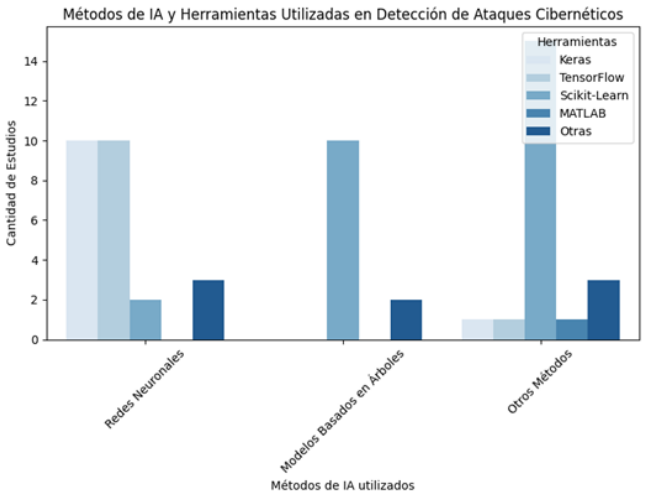

Fig. 3. Métodos de IA y Herramientas utilizadas

C. ¿Qué niveles de eficiencia han mostrado los métodos basados en inteligencia artificial en tasas de detección?

Los métodos basados en inteligencia artificial han mostrado altos niveles de eficiencia en la detección de ataques cibernéticos, con tasas de detección que alcanzan y, en algunos casos, superan el 90%. Un estudio logró una precisión del 99.78% empleando un modelo de bosque aleatorio, mientras que modelos de ensamble obtuvieron tasas cercanas al 99.7% [21]. Otro enfoque híbrido, que combinó técnicas de aprendizaje profundo y máquinas de soporte vectorial, reportó un 98.9% de precisión en la detección de phishing [22]. Asimismo, una arquitectura que utilizó redes neuronales profundas (DNN) logró una precisión de hasta el 97.95% [18], y una técnica de detección de bots basada en aprendizaje no supervisado alcanzó un 99.2% en precisión [23]. Adicionalmente, otro modelo con aprendizaje adaptativo alcanzó una tasa de detección del 94% para ejemplos maliciosos y del 81% para benignos, mostrando un rendimiento robusto en distintos escenarios [24]. Estos

resultados destacan la efectividad de los enfoques de IA (Inteligencia Artificial), especialmente aquellos basados en métodos híbridos y redes neuronales profundas, en mejorar la precisión y rapidez de la detección de amenazas en línea. Estas diferentes tasas de detección se muestran en la Tabla V y en la Figura 4 se muestra la distribución de modelos según su tasa de detección: 12 modelos en el rango de 99 % a 100 %, 8 modelos en el rango de 95 % a 98.99 %, 3 modelos en el rango de 90 % a 94.99 %, y 3 modelos con tasas menores a 89.99 %.

TABLA V
TASAS DE DETECCIÓN DE LOS MODELOS UTILIZADOS

Rango	**Modelos**	**Cantidad**
Menores de 89.99%	Regresión Logística (87.6%), BERT (67.41%), Clasificador (81%)	3
90 % - 94.99%	Bosque Aleatorio (94.7%), Apilamiento CNN (94.44%), Modelo (94%)	3
95 % - 98.99%	Bosque Aleatorio (95.3%), Modelo (95%), CNN (98.74%), CNN Propuesto (98.77%), Modelos (98.07% - 98.9%)	8
99 % - 100%	Bosque Aleatorio (99.78%), Ensamble (99.7%), Árbol de Decisión (99%), Bosque Aleatorio (99.5% - 100%), Híbrido (99.8%), Modelos (99% - 100%)	12

FUENTE: ELABORACIÓN PROPIA

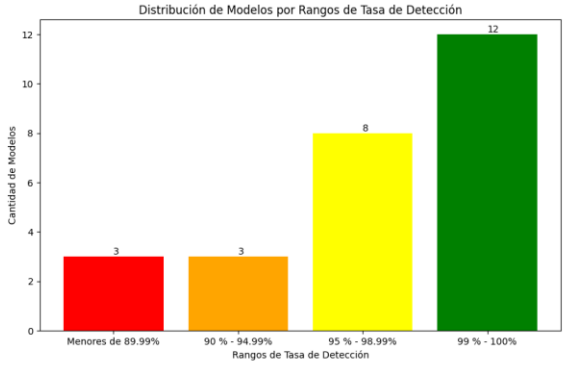

Fig. 4. Tasas de Detección de los Modelos utilizados

D. ¿En qué tipos de sitios web se ha investigado la detección de ataques cibernéticos?

En la investigación sobre detección de ataques cibernéticos, se ha analizado una variedad de tipos de sitios web para mejorar la eficacia de los modelos de detección en distintos contextos. Principalmente, se han investigado sitios legítimos y de phishing, con fuentes de datos comunes como PhishTank, Common Crawl, Alexa y bases de datos específicas para phishing como PhishTank y Kaggle, proporcionando URLs benignas y maliciosas [8]. Varios estudios se centraron en aplicaciones web con contenido malicioso y benigno, como los sitios de alto perfil en Alexa y sitios con vulnerabilidades específicas, incluyendo muestras de bases de datos de seguridad como Snyk, Node Security Project y XSSed [9], [10]. Además, otros estudios han evaluado URLs maliciosas y benignas de PhishTank y MillerSmiles, utilizando entornos controlados para medir la efectividad de los modelos en escenarios realistas [19].

A continuación, en la Tabla VI se describen los tipos de sitios web y su acceso los cuales fueron evaluados en los diferentes artículos ya especificados en la investigación.

TABLA VI
TIPOS SITIOS WEB EVALUADOS

Categoria de Sitio	Autores (Estudios)	Tipo de Acceso
Phishing y Legítimos	Sahingoz et al., Sanpra et al., Alhamyani et al., Saleem et al., Abu Al-Haija Q., Aldakheel et al., Wang et al., Sánchez-Paniagua et al., Shaiba et al., Hossain et al.	Público / No Especificado
Solo Phishing	Almousa et al., Yang et al., Odeh et al.	Público
Sitios Gubernamentales	Ajhari et al.	Público
Redes Sociales	Terumalasetti et al.	Público
Sitios Comerciales	Tastoush et al., Rovetta et al.	Público
Solo Legítimos	Alazab et al.	Público
No Especificado / General	Sheenamer et al., Lugbih et al., Oladipo et al.	Público / No Especificado

FUENTE: ELABORACIÓN PROPIA

De igual forma, en la Figura 5 se detalla la cantidad referente a los tipos de sitios web.

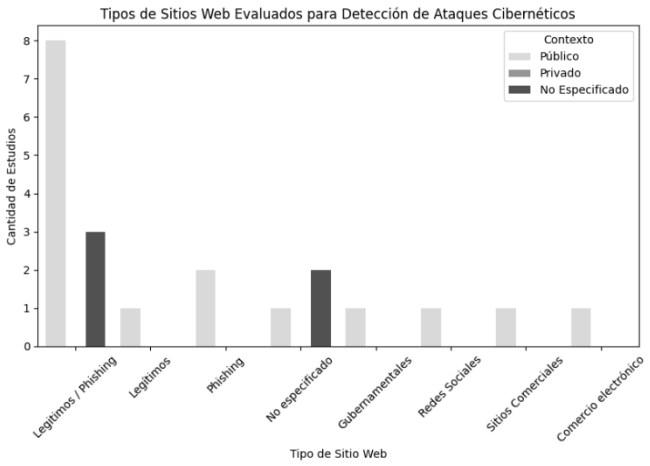

Fig. 5. Tipos de Sitios Web Evaluados para Detección de Ataques Cibernéticos

IV. DISCUSIÓN

En el presente estudio de revisión, los principales hallazgos demuestran una amplia variedad de ataques cibernéticos que afectan a los sitios web, destacando el phishing y la suplantación de identidad como las amenazas más frecuentemente investigadas, con una frecuencia total de 21 estudios [8], [9]. Este resultado corrobora lo señalado por Sahingoz et al., quienes identificaron el phishing como el ataque más prevalente debido a su capacidad para engañar a los usuarios y comprometer datos sensibles [8]. Sin embargo, en contraposición, los ataques basados en inyecciones de código, como el Cross-Site Scripting (XSS) y las inyecciones SQL, también presentan un impacto significativo al explotar vulnerabilidades en aplicaciones web, una tendencia respaldada por estudios como los de Wang et al. y Alhamyani et al. [10], [11]. Por consiguiente, estos hallazgos reflejan la necesidad de enfoques integrales de seguridad que aborden tanto las vulnerabilidades técnicas como los vectores de engaño social.

En términos de métodos de detección, los avances en inteligencia artificial (IA) han jugado un papel crucial, destacando las redes neuronales convolucionales (CNN) y los modelos de bosque aleatorio como herramientas altamente eficientes. Por ejemplo, los resultados de estudios como los de Sánchez-Paniagua et al. corroboran esta efectividad. logrando una precisión del 99.78% empleando bosques aleatorios, lo que subraya la efectividad de estos métodos en la detección de URLs maliciosas [21]. Este resultado se alinea con las investigaciones de Abu Al-Haija, que demuestran cómo las técnicas de aprendizaje profundo pueden superar los enfoques tradicionales en términos de precisión [22]. En contraposición, algunos modelos, como los basados en BERT (Representaciones Codificadoras Bidireccionales a partir de Transformadores), reportaron menores tasas de detección, con un rendimiento de apenas el 67.41% [23], lo que sugiere que la elección del modelo y la calidad de los datos de entrenamiento son factores determinantes en la efectividad.

Comparando los niveles de eficiencia, se constata que los modelos híbridos y los enfoques basados en redes neuronales profundas muestran un rendimiento significativamente superior, con tasas de detección que superan el 99% en múltiples estudios [21], [24]. Esto contrasta, no obstante, con las técnicas tradicionales basadas en árboles de decisión, que, aunque efectivas en ciertos casos, tienden a ser menos precisas en escenarios complejos [9], [10]. Esta diferencia puede explicarse por la capacidad de las redes neuronales para procesar grandes volúmenes de datos y capturar patrones complejos que los modelos más simples no pueden identificar.

A pesar de los avances, existen limitaciones en los estudios analizados. En primer lugar, muchos de los modelos se evaluaron en entornos controlados, lo que corrobora las observaciones de Oladipo et al., quienes señalaron que la falta de representatividad de los datos utilizados podría haber influido en la precisión reportada [12]. Además, la dependencia de conjuntos de datos públicos, como PhishTank y Alexa, introduce un sesgo, ya que estos pueden no representar adecuadamente el panorama completo de las amenazas [8], [9].

En cuanto a las implicancias, estos hallazgos subrayan, por una parte, la importancia de desarrollar soluciones basadas en IA que puedan adaptarse a diferentes tipos de sitios web, desde aplicaciones comerciales hasta redes sociales, como lo sugieren las investigaciones de Terumalasetti et al. [19]. Por otra parte, remarcan la necesidad de combinar métodos tradicionales y avanzados para abordar las limitaciones individuales y mejorar la robustez de los sistemas de detección.

Para futuras investigaciones, se recomienda explorar enfoques que integren aprendizaje no supervisado y modelos generativos para identificar patrones emergentes en ataques cibernéticos. Asimismo, sería valioso analizar cómo la integración de datos en tiempo real puede mejorar la efectividad de los modelos en escenarios dinámicos. También se sugiere investigar la interoperabilidad entre modelos para diseñar sistemas más resilientes que puedan enfrentar múltiples tipos de amenazas de manera simultánea.

En conclusión, aunque los avances en IA han permitido importantes progresos en la detección de ataques cibernéticos, persisten desafíos relacionados con la generalización de los modelos y la representatividad de los datos. Superar estas limitaciones será esencial para mejorar la seguridad de los sitios web en un panorama de amenazas en constante evolución.

V. CONCLUSIONES

La presente revisión sistemática de literatura ha cumplido con el objetivo de identificar las prácticas actuales más efectivas en el campo de la protección eficaz, permitiendo establecer una visión integral y actualizada de los métodos disponibles. Los hallazgos destacan que las estrategias más

exitosas se basan en enfoques adaptativos, tecnologías emergentes y metodologías centradas en la prevención activa.

De acuerdo con los resultados obtenidos, se identificaron patrones clave en las prácticas más efectivas, como la implementación de sistemas dinámicos que responden a cambios contextuales y la integración de herramientas analíticas avanzadas para predecir y mitigar riesgos. Estas estrategias han demostrado ser altamente relevantes en escenarios donde los riesgos evolucionan rápidamente, ofreciendo una base sólida para futuras aplicaciones.

La contribución de esta revisión radica en ofrecer un panorama exhaustivo que consolida los avances recientes en el área, estableciendo un punto de referencia para investigaciones posteriores. Al brindar una síntesis estructurada de la literatura existente, este trabajo facilita la identificación de brechas de conocimiento y oportunidades para el desarrollo de soluciones innovadoras y más robustas, contribuyendo de manera significativa al estudio y mejora continua en este campo.

REFERENCIAS

[1] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol. 7, pp. 10127-10149, 2019. DOI: 10.1109/ACCESS.2018.2890507

[2] T. Alharbi, A. K. S. Perera, S. Alshamrani, "Multi-SpacePhish: Extending the Evasion-space of Adversarial Attacks against Phishing Website Detectors Using Machine Learning," Proceedings of the 33rd ACM SIGSAC Conference on Computer and Communications Security, Oct. 2024, pp. 150-162. DOI:10.1145/3638253

[3] A. Kummar., M. Agarwal., "Quick service during DDoS attacks in the container-based cloud environment," Journal of Network and Computer Applications, vol. 220, pp. 103946, Jan. 2024. DOI: 10.1016/j.jnca.2024.103946

[4] N. Kamble, N. Mishra, "Hybrid optimization enabled squeeze net for phishing attack detection," Computers & Security, vol. 131, pp. 103901, Feb. 2024. DOI: 10.1016/j.cose.2024.103901

[5] A. Singh, P. K. Singh, "SmartiPhish: a reinforcement learning-based intelligent anti-phishing solution to detect spoofed website attacks," International Journal of Information Security, vol. 23, no. 5, pp. 789-805, Jul. 2023. DOI: 10.1007/s10207-023-00778-9

[6] C. M. da C. Santos, C. A. de M. Pimentaand M. R. C. Nobre, "The PICO strategy for the research question construction and evidence search", Rev. Latino-Am. Enfermagem, vol. 15, no. 3, pp. 508–511, Jun. 2007, doi: 10.1590/S0104-11692007000300023.

[7] Page, M. J.; McKenzie, J. E.; Bossuyt, P. M.; Boutron, I., Hoffmann, T. C.; Mulrow, C. D.; Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic The BMJ, 372 DOI:10.1136/bmj.n71

[8] O. K. Sahingoz, et al., "DEPHIDES: Deep Learning Based Phishing Detection System," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3352629

[9] [9] E. Sangra, et al., "Malicious Website Detection Using Random Forest and Pearson Correlation," International Journal of Advanced Computer Science and Applications, 2024. DOI: 10.14569/IJACSA.2024.0150876

[10] R. Alhamyani, et al., "Machine Learning-Driven Detection of Cross-Site Scripting Attacks," Information (Switzerland), 2024. DOI: 10.3390/info15070420

[11] A. Sheneamer, "Vulnerable JavaScript functions detection using stacking of convolutional neural networks," PeerJ Computer Science, 2024. DOI: 10.7717/peerj-cs.1838

[12] H. Lughbi, et al., "CybAttT: A Dataset of Cyberattack News Tweets for Enhanced Threat Intelligence," Data, 2024. DOI: 10.3390/data9030039

[13] A. S. Saleem Raja, et al., "Natural language based malicious domain detection," Scientific and Technical Journal of Information Technologies, 2023. DOI: 10.17586/2226-1494-2023-23-2-304-312

[14] Q. Abu Al-Haija, "Cost-effective detection system of cross-site scripting attacks," Results in Engineering, 2023. DOI: 10.1016/j.rineng.2023.101266

[15] I. D. Oladipo, et al., "A Secure and Scalable Behavioral Dynamics Authentication Model," International Journal of Advanced Computer Science and Applications, 2023. DOI: 10.14569/IJACSA.2023.0140804

[16] D. M. Uliyan, B. N. Almousa, "Anti-Spoofing in Medical Employee's Email," Sensors, 2023. DOI: 10.14569/IJACSA.2023.0140727

[17] A. A. Ajhari, et al., "PROCTOR: A Robust URL Protection System," International Journal of Computing and Digital Systems, 2023. DOI: 10.12785/IJCDS/140179

[18] E. A. Aldakheel, et al., "A Deep Learning-Based Innovative Technique for Phishing Detection," Sensors, 2023. Doi: 10.3390/s23094403

[19] Odeh A., Keshta I., Abdelfattah E., "Phiboost - A Novel Phishing Detection Model Using Adaptive Boosting Approach," Jordanian Journal of Computers and Information Technology, 2021. DOI: 10.5455/jjcit.71-1600061738.

[20] Terumalasetti S., Reeja S.R., "A Sophisticated Deep Learning Framework of Advanced Techniques to Detect Malicious Users in Online Social Networks," International Journal of Advanced Computer Science and Applications, 2023. DOI: 10.14569/IJACSA.2023.0141264.

[21] Wang Y., Ma W., Xu H., Liu Y., Yin P., "A Lightweight Multi-View Learning Approach for Phishing Attack Detection Using Transformer with Mixture of Experts," Applied Sciences (Switzerland), 2023. DOI: 10.3390/app13137429.

[22] M. Sánchez-Paniagua et al., "A Classifier to Detect Profit and Non-Profit Websites Upon Textual Metrics for Security Purposes," J. ICT Res. Appl., 2022. Doi: 10.5614/itbj.ict.res.appl.2022.16.1.6

[23] S. Rovetta, G. Suchacka, y F. Masulli, "Bot recognition in a Web store: An approach based on unsupervised learning," Comput. Mater. Continua, 2022. DOI: 10.1016/j.jnca.2020.102577

[24] H. Shaiba et al., "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," Jordanian J. Comput. Inf. Technol., 2021. DOI:10.3390/s21248281