Diagnóstico del desempeño de modelos de aprendizaje automático para la detección de sitios web de phishing: Una revisión de literatura

Santa Cruz-Rufasto, Frank Luis[1], Dios-Castillo, Christian Abraham[2],
[12]Universidad Tecnológica del Perú, Perú, U21229982@utp.edu.pe, C16763@utp.edu.pe

Abstract- Detecting phishing websites using Machine Learning (ML) techniques is a key approach in modern cybersecurity, with models such as Random Forest reaching accuracy levels close to 99%, followed by Support Vector Machine, Decision Tree and Logistic Regression. However, what is the level of accuracy of ML techniques in this task and what are the key factors affecting their accuracy and effectiveness? The results highlight that the quality and diversity of the training data, together with metrics such as Accuracy, Precision and Recall, are determinants in the performance of the models. In addition, the ability of algorithms to adapt to dynamic attack patterns is crucial. This study, based on a systematic review with the PRISMA statement, analyzed 43 articles selected from more than 4,600 initials, revealing the importance of developing computationally efficient methods that maintain high levels of accuracy to address growing digital threats.

Keywords-- Phishing detection, Machine Learning, Random Forest, Cybersecurity, Precision metrics.

Diagnóstico del desempeño de modelos de aprendizaje automático para la detección de sitios web de phishing: Una revisión de literatura

Santa Cruz-Rufasto, Frank Luis[1], Dios-Castillo, Christian Abraham[2],
[12]Universidad Tecnológica del Perú, Perú, U21229982@utp.edu.pe, C16763@utp.edu.pe

Resumen- ***La detección de sitios web de phishing mediante técnicas de Machine Learning (ML) es un enfoque clave en la ciberseguridad moderna, con modelos como Random Forest alcanzando niveles de precisión cercanos al 99%, seguidos por Support Vector Machine, Decision Tree y Logistic Regression. Sin embargo, ¿cuál es el nivel de precisión de las técnicas de ML en esta tarea y cuáles son los factores clave que afectan su precisión y efectividad? Los resultados destacan que la calidad y diversidad de los datos de entrenamiento, junto con métricas como Accuracy, Precision y Recall, son determinantes en el rendimiento de los modelos. Además, la capacidad de los algoritmos para adaptarse a patrones dinámicos de ataques resulta crucial. Este estudio, basado en una revisión sistemática con la declaración PRISMA, analizó 43 artículos seleccionados de más de 4,600 iniciales, revelando la importancia de desarrollar métodos computacionalmente eficientes que mantengan altos niveles de precisión para afrontar las crecientes amenazas digitales.***

Palabras clave-- ***Detección de phishing, Aprendizaje automático, Random Forest, Ciberseguridad, Métricas de precisión.***

I. INTRODUCCIÓN

En la era digital, la proliferación de sitios web de phishing representa una amenaza creciente tanto para usuarios individuales como para organizaciones [1]. Estas páginas fraudulentas, diseñadas para imitar sitios legítimos, buscan capturar información sensible de sus víctimas, como credenciales de acceso y datos financieros [2]. Frente a este desafío, las técnicas de Machine Learning (ML) han emergido como herramientas prometedoras en la detección automática de phishing, ofreciendo potencial para mejorar la precisión y la velocidad en la identificación de estos sitios web [3]. Sin embargo, la eficacia de estas técnicas varía considerablemente en función de múltiples factores, tales como el tipo de algoritmo utilizado, la calidad y diversidad de los datos de entrenamiento, y los patrones específicos que caracterizan a los ataques de phishing en constante evolución [4]. Este estudio se enfoca en analizar la precisión de diversas metodologías de ML aplicadas en este contexto, evaluando además los factores clave que influyen en su rendimiento. Esta revisión busca proporcionar una visión detallada y actualizada del estado del arte en técnicas de detección de phishing basadas en ML, destacando oportunidades para optimizar su efectividad y responder a las necesidades de seguridad digital actuales [2]. El dinámico ámbito de la ciberseguridad, caracterizado por amenazas cada vez más complejas y variadas, el uso del aprendizaje automático (ML) ha surgido como un factor crucial para fortalecer las medidas de seguridad digital. El ML permite a los expertos en ciberseguridad examinar grandes cantidades de información, identificar irregularidades y pronosticar riesgos potenciales en tiempo real. Esta tecnología innovadora no solo mejora la eficiencia y precisión en la identificación de amenazas potenciales, sino que también permite tomar medidas proactivas en respuestas a la aparición de ciberpeligrosos [5, 6]. El uso irresponsable de las redes sociales y el desconocimiento de las vulnerabilidades de los ataques de phishing hacen que los ataques aumenten constantemente. Los cibercriminales pueden atacar a los usuarios obteniendo información de sus cuentas o contactos mediante phishing a través de spam [7]. Esta investigación se justifica en la necesidad de analizar literatura especializada que permita comprender la forma de mejorar la ciberseguridad y proteger la información personal, como uno de los mayores desafíos del mundo. Cuando se desarrollan nuevas tecnologías web como la computación en la nube, la computación móvil, el comercio electrónico, la banca en línea, etc., es necesario pensar en cómo proteger a los usuarios. Los gobiernos piensan en los “delitos cibernéticos”, que aumentan en las actividades diarias y crean agujeros de ataque para que los atacantes los exploten [8].

II. METODOLOGIA

Este estudio se desarrolló a través de una revisión sistemática de la literatura, utilizando un enfoque estructurado que garantizara precisión tanto en la formulación de la pregunta de investigación como en la estrategia de búsqueda y selección de artículos. Se establecieron los elementos esenciales del análisis para definir claramente el alcance y maximizar la recopilación de estudios relevantes. Esto permitió asegurar que los estudios incluidos fueran completos y adecuados para responder a los objetivos de la investigación, lo cual abarca la siguiente pregunta principal ¿Cuál es el nivel de precisión de las técnicas de Machine Learning en la detección de sitios web de phishing, y cuáles son los factores clave que influyen en su precisión y efectividad?, esta primera pregunta se enfoca

en identificar los criterios utilizados en la detección de sitios web de phishing, proporcionando una base clara para la evaluación del problema. La segunda pregunta explora las características y los enfoques de los modelos más utilizados, destacando las técnicas implementadas para abordar este desafío. Finalmente, la tercera pregunta analiza los modelos con mayor precisión reportada, evaluando su efectividad y desempeño en la práctica.

Este enfoque metodológico permite establecer un marco que facilita la comprensión integral del tema, definiendo con claridad las variables de estudio, los métodos empleados y los resultados esperados. Además, proporciona una estructura que no solo permite identificar los métodos más efectivos, sino también evaluar su impacto y aplicabilidad en el contexto actual de la ciberseguridad. En la tabla I se muestran las preguntas específicas y las palabras claves que se utilizaron en la ecuación de búsqueda, la cual fue diseñada empleando cadenas interconectadas por operadores booleanos, tales como **"AND"** y **"OR"**, optimizando la recuperación de documentos relevantes en bases de datos científicas.

TABLA I
PREGUNTAS Y PALABRAS CLAVES

N°	PREGUNTA	PALABRAS CLAVE
1	¿Cuáles son los criterios en la detección de sitios web de phishing?	Phishing detection, websites, detection criterio, phishing websites
2	¿Qué modelos de Machine Learning son más precisos en la detección de Phishing?	Machine Learning models, phishing detection, accuracy, best models
3	¿Cuál es el nivel de efectividad en los diferentes modelos de Machine Learning en la detección de Phishing?	Machine Learning models, phishing detection, effectiveness, performance evaluation

Se utilizaron las bases de datos Scopus y Web of Science (WoS). Para ello se realizó una búsqueda automatizada de términos clave relacionado con la detección de sitios web de phishing y el uso de modelos de Machine Learning. La cadena de búsqueda utilizada fue: (TITLE-ABS-KEY ("phishing" OR "websites" OR "Online platform") AND TITLE-ABS-KEY ("machine learning" OR "Learning algorithms") AND TITLE-ABS-KEY ("presicion" OR "efficiency" OR "accuracy")) AND PUBYEAR > 2022 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (OA , "all")). Se incluyen los filtros debido a que la información inicialmente obtenida fue mayor a 4,000 documentos de todo tipo.

Para seleccionar y filtrar los artículos relevantes, se utilizó la declaración PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), la cual proporciona una guía estructurada y transparente para la revisión de literatura científica y garantiza que el proceso de selección sea claro y reproducible [9]. PRISMA facilita la identificación y exclusión de estudios no pertinentes mediante la aplicación de criterios de inclusión y exclusión previamente definidos, los cuales se detallan en la Tabla II, asegurando que solo se incluyan aquellos estudios que cumplan con los objetivos específicos de esta investigación.

TABLA II
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

CRITERIOS DE INCLUSIÓN	CRITERIOS DE EXCLUSIÓN
CI1: Los trabajos de investigación incluidos deben abordar el tema de la detección de sitios web de phishing.	CE1: Trabajos de investigación que no estén disponibles en acceso abierto.
CI2: Los trabajos de investigación deben aplicar técnicas de Machine Learning en la detección de phishing.	CE2: Publicaciones en idiomas diferentes al inglés.
CI3: Los trabajos de investigación deben estar disponibles en formato PDF y ser de acceso abierto.	CE3: Excluir otros tipos de trabajo de investigación que no sean artículos científicos.
CI4: Los trabajos de investigación deben estar relacionados con las áreas temáticas de ciberseguridad y Machine Learning.	CE4: Estudios no relacionadas con la ciberseguridad o detección de phishing mediante Machine Learning.
CI5: Los trabajos de investigación deben haber sido publicados entre los años 2023 y 2024.	CE5: Trabajo de investigación anteriores a 2023 o después de 2024.

Después de la identificación de 460 artículos obtenidos en las bases de datos Scopus y Web of Science el día 30/09/2024 a las 9:50 A.M, se obtuvo un total de 4653 artículos. Para asegurar la transparencia, exhaustividad y reproducibilidad en la selección de estudios relevantes, se decidió llevar a cabo un proceso de revisión estructurada siguiendo las pautas de la declaración PRISMA. Este protocolo se basa en un proceso de filtrado en dos etapas que facilita la selección precisa de los artículos relevantes para el estudio.

En la primera etapa, se aplicaron filtros iniciales conforme a los criterios de inclusión y exclusión establecidos, evaluando aspectos como el título, el resumen, el idioma de publicación, el tipo de documento y el año de publicación. Posteriormente, se realizó una segunda etapa de filtrado en la que se revisó el texto completo de los artículos para asegurar el cumplimiento de estos criterios. De los 4653 artículos iniciales, se excluyeron un total de 4193 publicaciones por varias razones específicas: 3225 no eran de acceso abierto, 283 no correspondían al tipo de documento requerido (no eran artículos), 5 estaban en idiomas distintos al inglés y 680 estaban fuera del periodo de 2023 a 2024. Esto resultó en una selección preliminar de 460 artículos

potencialmente relevantes, de los cuales 358 fueron de Scopus y 102 de Web Of Science.

Luego de esta primera fase de filtrado, se identificaron y eliminaron 93 artículos duplicados entre ambas bases de datos. Posteriormente, se revisaron los títulos y resúmenes de los artículos restantes, descartándose 256 por no estar directamente relacionados con el tema de estudio. Asimismo, se excluyeron 5 artículos no cumplían con los criterios de acceso abierto y 63 más porque el contenido completo no guardaba relación con el enfoque de investigación. Al concluir esta segunda fase de revisión, se seleccionaron 43 artículos finales para la revisión detallada.

Este proceso de selección se llevó a cabo de manera estructurada y rigurosa, asegurando la inclusión de estudios relevantes y de alta calidad. Todo el procedimiento se ha sintetizado en el diagrama PRISMA, el cual ilustra visualmente las etapas clave del proceso, incluyendo la búsqueda inicial, la eliminación de duplicados, la exclusión de estudios no pertinentes y la selección final de artículos relevantes.

Este enfoque, basado en la declaración PRISMA, se apoya en una guía especializada para la realización de revisiones sistemáticas de literatura, garantizando que los informes sean transparentes, completos y precisos. La declaración PRISMA 2020, una actualización de 2009 proporciona pautas mejoradas sobre cómo estructurar y presentar los informes, incluyendo una lista de 27 elementos clave, recomendaciones específicas y diagramas de flujo que son fundamentales para este tipo de estudios. Estas mejoras permiten aumentar la calidad de los informes en áreas como la detección de sitios web de phishing mediante técnicas de Machine Learning, facilitando la construcción sobre investigaciones previas y simplificando la realización y actualización de revisiones, garantizando así evaluaciones más rigurosas de los estudios y metaanálisis [10].

El uso de Prisma no solo asegura la transparencia y exhaustividad en la selección de estudios, sino que también se ajusta a los estándares actualizados en presentación de informes en revisiones sistemáticas, beneficiando a la comunidad científica en general [11],[12].

TABLA PRISMA

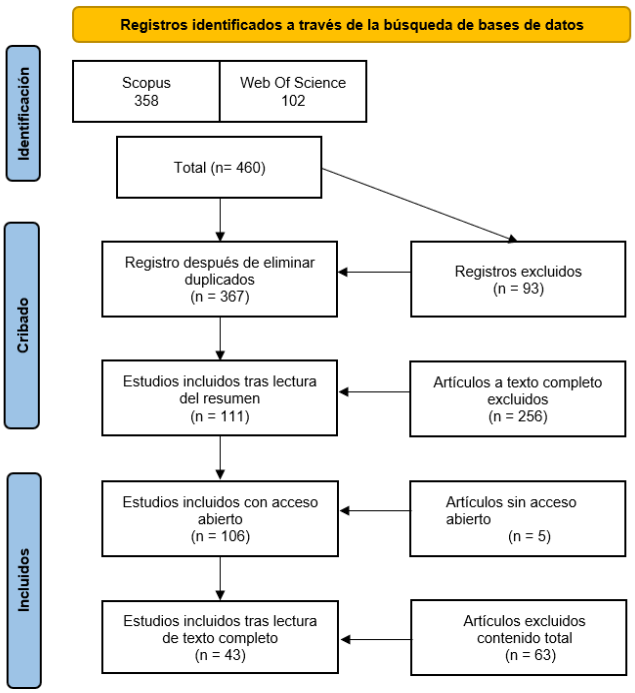

Figura 1 Diagrama Prisma

Nota: Elaborado a partir de los documentos analizados

La hoja de trabajo se encuentra en el siguiente enlace: https://zenodo.org/records/15304455

III. RESULTADOS Y DISCUSIONES

Este estudio presenta una recopilación y análisis detallado de artículos científicos, categorizados por fecha de publicaciones relacionadas con la detección de sitios web de phishing. Como se observa en la Figura 2, el análisis de las publicaciones revela una tendencia decreciente en los años más recientes. En 2023 se registraron 24 publicaciones mientras que en 2024 esta cifra disminuyó a 19 publicaciones. Aunque actualmente se observa una ligera disminución en 2024, este dato corresponde a la fecha de redacción del manuscrito y se espera un incremento al finalizar la indización del año 2024, destacando así la relevancia continua del tema en la investigación.

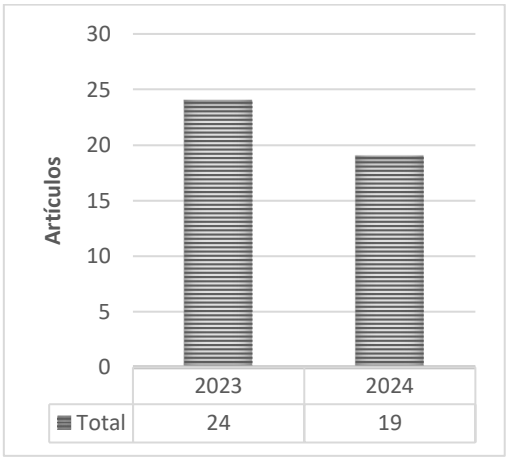

Figura 2 N° Artículos encontrados por año

Nota: Elaborado a partir de los documentos analizados.

Al analizar la distribución radial según como se observa en la figura 3, las investigaciones sobre detección de sitios web de phishing, se evidencia una clara concentración en ciertos países. India emerge como el líder indiscutible en este campo, contribuyendo con el 18% de los estudios analizados y teniendo el primer lugar en la cantidad de artículos que nos ayudara en el desarrollo de este review.

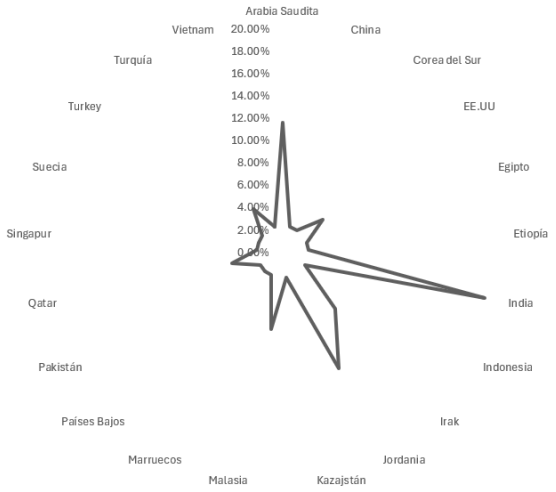

Figura 3 Artículos por país de publicación

Nota: Elaborado a partir de los documentos analizados.

En el contexto de los estudios analizados, se han identificado múltiples criterios de evaluación utilizados para medir la efectividad de los modelos de Machine Learning en la detección de sitios web de phishing. Estos criterios incluyen medidas como Accuracy, F1-score, Recall, y Precisión, que son las métricas más frecuentemente reportadas. Adicionalmente, se mencionan métricas como la Tasa de Falsos Positivos (FPR), AUC-ROC, Tasa de Falsos Negativos (FNR) y Coeficiente de Correlación de Matthews (MCC), aunque con menor frecuencia. En la Tabla III de este análisis se identificar las métricas prioritarias y complementarias en el contexto de evaluación de modelos para phishing.

TABLA III
CRITERIOS DE PORCENTAJE MÁS ALTO

CRITERIOS	%PROMEDIO	ID REFERENCIA
Accuracy	76.74%	[14],[15],[16],[17],[19],[20],[23],[25],[26],[27],[28],[29],[32],[34],[36],[38],[39],[40],[41],[42],[43],[44],[45],[46],[47],[48],[49],[50],[51],[52],[54],[55],[56]
F1-score	55.81%	[14],[17],[20],[25],[26],[27],[28],[29],[32],[33],[38],[39],[40],[41],[42],[43],[44],[45],[47],[50],[51],[52],[54],[56]
Recall	48.84%	[17],[20],[25],[26],[28],[29],[32],[33],[39],[40],[41],[42],[43],[44],[45],[49],[50],[51],[52],[55],[56]
Precisión	53.49%	[18],[20],[22],[26],[28],[29],[32],[33],[36],[39],[40],[41],[42],[43],[44],[45],[49],[50],[51],[52],[54],[55],[56]
FPR	11.63%	[14],[15],[23],[40],[44]
AUC-ROC	9.30%	[14],[17],[23],[47]
FNR	9.30%	[14],[15],[23],[40]
MCC	2.33%	[19]

Nota: Elaborado a partir de los documentos analizados.

La primera pregunta específica que se logró plantear en esta investigación fue: ¿Cuáles son los modelos de aprendizaje más utilizados en la detección de sitios web de phishing?

El análisis de los artículos que se muestra en la Figura 4, muestra una preferencia estadísticamente significativa por Machine Learning como modelo más utilizado. Este indicador, que mide la detección de sitios web de phishing, es utilizado en el 45% de los artículos, posicionándose por encima de otros modelos como Deep Learning y Análisis de URL. Este resultado demuestra que los investigadores se enfocaron en la forma de implementar este factor en las computadoras, dando lugar a un nuevo subcampo de la inteligencia artificial conocido como aprendizaje automático (ML). Este tipo de algoritmo permite realizar predicciones sobre eventos futuros sin depender de reglas o modelos predefinidos, desarrollar modelos que expliquen los comportamientos de entidades en el mundo real e identificar patrones a partir de los datos recopilados [15].

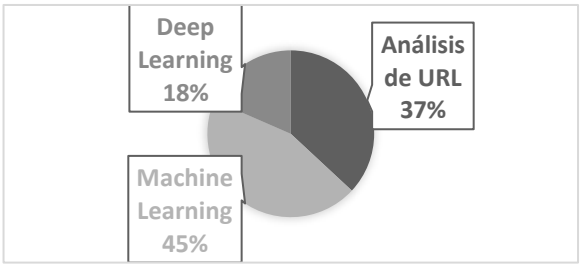

Figura 4 Modelos de aprendizaje en la detección de phishing

Nota: Elaborado a partir de los documentos analizados.

La segunda pregunta especifica que planteamos en esta investigación es: ¿Qué modelos de Machine Learning son los más comunes y mayor Accuracy en la detección de Phishing?

De todos los 43 artículos leídos la Figura 5 muestra la precisión de cuatro modelos de Machine Learning más comunes y con mayor precisión utilizados en la detección de sitios web de phishing: Random Forest (RF), Decision Tree (DT), Logistic Regression (LR) y Support Vector Machine (SVM). Random Forest destaca con la mayor precisión, superando el 99%, seguido por SVM, Decision Tree y Logistic Regression presentan resultados más bajos. Esto sugiere que Random Forest es el modelo más preciso, mientras que los demás ofrecen una precisión ligeramente inferior, aunque aún son útiles en la clasificación de sitios de phishing.

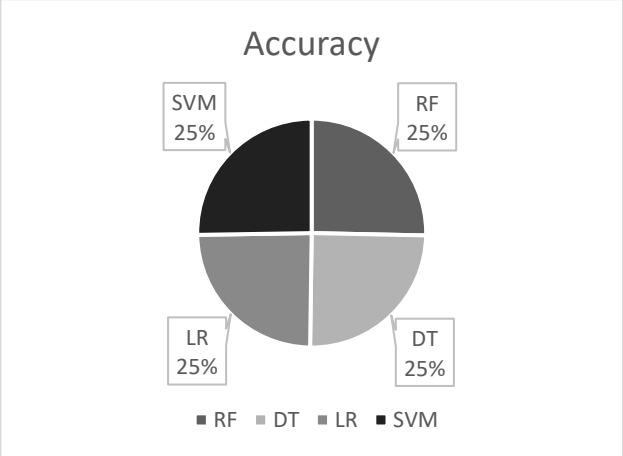

Figura 5 Modelos más comunes y con mayor precisión en la detección de sitios web de phishing

Nota: Elaborado a partir de los documentos analizados.

La tercera pregunta especifica que planteamos en esta investigación es: ¿Cuál es el nivel de efectividad en los diferentes modelos de Machine Learning en la detección de Phishing?

La Figura 6 presenta de manera clara cómo los distintos modelos de Machine Learning utilizados para detectar sitios web de phishing se desempeñan en términos de precisión. Se observa que el modelo RF (Random Forest) sobresale significativamente, alcanzando un nivel de precisión cercano al 100%. Esto sugiere que el RF es altamente efectivo en la identificación de sitios web fraudulentos. Sin embargo, es importante considerar que la elección del modelo óptimo puede variar dependiendo del conjunto de datos y los requisitos específicos de cada aplicación.

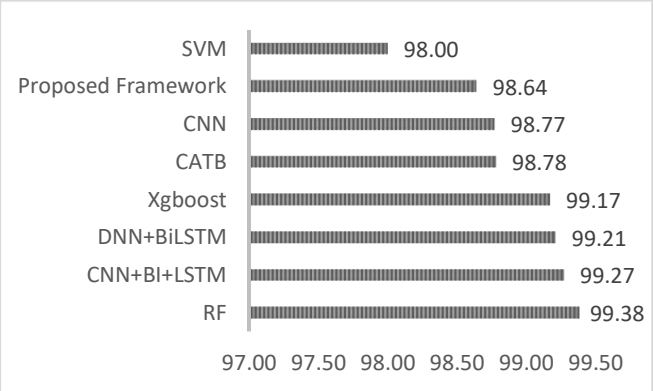

Figura 6 Modelos con mayor Acurracy

Nota: Elaborado a partir de los documentos analizado

IV. Conclusiones

Tras el análisis realizado en este RSL, se identificó que los modelos de Machine Learning más utilizados para la detección de sitios web de phishing son Random Forest, Support Vector Machine, Logistic Regression y Decision Tree, debido a su capacidad de aprendizaje supervisado y efectividad en la clasificación de datos. Entre las métricas más empleadas para evaluar el desempeño de estos modelos destacan Accuracy, Precision, Recall y F1-score, lo que evidencia la importancia de analizar el rendimiento desde múltiples perspectivas para garantizar una detección confiable y precisa. Asimismo, se observó que la elección del modelo depende no solo de su efectividad, sino también de su capacidad para adaptarse a entornos con recursos computacionales limitados, considerando la creciente necesidad de implementar soluciones eficientes y accesibles en el ámbito de la ciberseguridad. Esto subraya la relevancia de continuar explorando enfoques más innovadores y ligeros para optimizar la detección de amenazas en sitios web de phishing.

V. AGRADECIMIENTO

Expresamos el agradecimiento al Dr. Nestor Abel Sánchez Goycochea (nsanchezg@utp.edu.pe) por su valiosa orientación y apoyo en el desarrollo de esta revisión sistemática de literatura.

VI. REFERENCIAS

[1] Jain, A. K., & Gupta, B. B. (2018). *Phishing detection: Analysis of visual similarity-based approaches*. *Security and Privacy*, *1*(2), e20. doi:10.1002/spy2.20.

[2] Verma, R., & Das, A. (2017). *What's in a URL: Fast Feature Extraction and Malicious URL Detection*. In *Proceedings of the 3rd ACM on International Workshop on Security and Privacy Analytics* (pp. 55-63). ACM. doi:10.1145/3041008.3041015.

[3] Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). *Phishing detection based associative classification data mining*. *Expert Systems with Applications*, *41*(13), 5948-5959. doi:10.1016/j.eswa.2014.03.019.

[4] Zhang, Z., & Yuan, X. (2018). *Phishing detection using machine learning techniques*. In *Proceedings of the ACM Southeast Conference* (pp. 1-8). ACM. doi:10.1145/3190645.3190652.

[5] T. Berghout, M. Benbouzid, and S. M. Muyeen, "Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects," *Int. J. Crit. Infrastruct. Prot.*, vol. 38, no. 19, pp. 100547, 2022. doi: 10.1016/j.ijcip.2022.100547.

[6] I. D. Aiyanyo, H. Samuel, and H. Lim, "A systematic review of defensive and offensive cybersecurity with machine learning," *Appl. Sci.*, vol. 10, no. 17, pp. 5811, 2020. doi: 10.3390/app10175811.

[7] MK Rogers, La psique de los cibercriminales: una perspectiva psicosocial. En: Cybercrimes: A Multidisciplinary Analysis. Berlín, Heidelberg: Springer, págs. 217–235, 2011.

[8] RM Rodríguez y A. Atyabi, "Ataques y defensas de ingeniería social en el mundo físico vs. ciberespacio: un estudio de contraste", Preprint ArXiv:2203.04813, págs. 1–26, 2022.

[9] 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 reviews. *BMJ*, *372*, n71. doi:10.1136/bmj.n71

[10] O'Dea, R. E., Lagisz, M., Jennions, M. D., Koricheva, J., Noble, D. W., Parker, T. H., Gurevitch, J., Page, M. J., Stewart, G., Moher, D., y Nakagawa, S., "Evolution of epistatic networks via quantum evolutionary computing," *Biological Reviews*, vol. 96, no. 5, pp. 1695-1722, Sep. 2021, doi: 10.1111/brv.12721.

[11] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," Syst Rev, vol. 10, no. 1, Dec. 2021, doi: 10.1186/s13643-021-01626-4

[12] R. E. O'Dea et al., "Preferred reporting items for systematic reviews and meta-analyses in ecology and evolutionary biology: a PRISMA extension," Biological Reviews, vol. 96, no. 5, pp. 1695–1722, Oct. 2021, doi: 10.1111/brv.12721.

[13] K. Adane, B. Beyene, and M. Abebe, "ML and DL-based Phishing Website Detection: The Effects of Varied Size Datasets and Informative Feature Selection Techniques," *J. Artif. Intell. Technol.*, vol. 4, no. 1, pp. 18–30, 2024, doi: 10.37965/jait.2023.0269.

[14] M. A. Tamal, M. K. Islam, T. Bhuiyan, A. Sattar, and N. U. Prince, "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning," *Front. Comput. Sci.*, vol. 6, no. January, 2024, doi: 10.3389/fcomp.2024.1428013.

[15] M. A. Taha, H. D. A. Jabar, and W. K. Mohammed, "A Machine Learning Algorithms for Detecting Phishing Websites: A Comparative Study," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 3, pp. 275–286, 2024, doi: 10.52866/ijcsm.2024.05.03.015.

[16] A. Ishtaiwi *et al.*, "Next-Gen Phishing Defense Enhancing Detection With Machine Learning and Expert Whitelisting/Blacklisting," *Int. J. Cloud Appl. Comput.*, vol. 14, no. 1, pp. 1–17, 2024, doi: 10.4018/IJCAC.353301.

[17] G. O. Boussi, H. Gupta, and S. A. Hossain, "A machine learning model for predicting phishing websites," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 4, pp. 4228–4238, 2024, doi: 10.11591/ijece.v14i4.pp4228-4238.

[18] S. Aslam, H. Aslam, A. Manzoor, H. Chen, and A. Rasool, "AntiPhishStack: LSTM-Based Stacked Generalization Model for Optimized Phishing URL Detection," *Symmetry (Basel).*, vol. 16, no. 2, 2024, doi: 10.3390/sym16020248.

[19] E. Sangra, R. Agrawal, P. R. Gundalwar, K. Sharma, D. Bangri, and D. Nandi, "Malicious Website Detection Using Random Forest and Pearson Correlation for Effective Feature Selection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 8, pp. 772–780, 2024, doi: 10.14569/IJACSA.2024.0150876.

[20] T. Swetha, M. Seshaiah, K. L. Hemalatha, S. V. N. Murthy, and M. B. H. Kumar, "Hybrid Machine Learning Approach for Real-Time Malicious URL Detection Using SOM-RMO and RBFN with Tabu Search," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 8, pp. 450–458, 2024, doi: 10.14569/IJACSA.2024.0150844.

[21] M. A. Elberri, Ü. Tokeşer, J. Rahebi, and J. M. Lopez-Guede, "A cyber defense system against phishing attacks with deep learning game theory and LSTM-CNN with African vulture optimization algorithm (AVOA)," *Int. J. Inf. Secur.*, vol. 23, no. 4, pp. 2583–2606, 2024, doi: 10.1007/s10207-024-00851-x.

[22] S. Das Guptta, K. T. Shahriar, H. Alqahtani, D. Alsalman, and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Ann. Data Sci.*, vol. 11, no. 1, pp. 217–242, 2024, doi: 10.1007/s40745-022-00379-8.

[23] D. M. Linh, H. D. Hung, H. M. Chau, Q. S. Vu, and T. N. Tran, "Real-time phishing detection using deep learning methods by extensions," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 3, pp. 3021–3035, 2024, doi: 10.11591/ijece.v14i3.pp3021-3035.

[24] S. Sankaranarayanan, A. T. Sivachandran, A. S. Mohd Khairuddin, K. Hasikin, and A. R. Wahab Sait, "An ensemble classification method based on machine learning models for malicious Uniform Resource Locators (URL)," *PLoS One*, vol. 19, no. 5, pp. 1–20, 2024, doi: 10.1371/journal.pone.0302196.

[25] P. K. K. Loh, A. Z. Y. Lee, and V. Balachandran, "Towards a Hybrid Security Framework for Phishing Awareness Education and Defense," *Futur. Internet*, vol. 16, no. 3, 2024, doi: 10.3390/fi16030086.

[26] R. J. van Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, "The applicability of a hybrid framework for automated phishing detection," *Comput. Secur.*, vol. 139, no. January, p. 103736, 2024, doi: 10.1016/j.cose.2024.103736.

[27] O. K. Sahingoz, E. Buber, and E. Kugu, "DEPHIDES: Deep Learning Based Phishing Detection System," *IEEE Access*, vol. 12, no. December 2023, pp. 8052–8070, 2024, doi: 10.1109/ACCESS.2024.3352629.

[28] O. Ussatova, A. Zhumabekova, V. Karyukin, E. T. Matson, and N. Ussatov, "The development of a model for the threat detection system with the use of machine learning and neural network methods," *Int. J. Innov. Res. Sci. Stud.*, vol. 7, no. 3, pp. 863–877, 2024, doi: 10.53894/ijirss.v7i3.2957.

[29] A. Ejaz, A. N. Mian, and S. Manzoor, "Life-long phishing attack detection using continual learning," *Sci. Rep.*, vol. 13, no. 1, pp. 1–14, 2023, doi: 10.1038/s41598-023-37552-9.

[30] D. Jibat, S. Jamjoom, Q. A. Al-Haija, and A. Qusef, "A Systematic Review: Detecting Phishing Websites Using Data Mining Models," *Intell. Converg. Networks*, vol. 4, no. 4, pp. 326–341, 2023, doi: 10.23919/ICN.2023.0027.

[31] S. Kapan and E. Sora Gunal, "Improved Phishing Attack Detection with Machine Learning: A Comprehensive Evaluation of Classifiers and Features," *Appl. Sci.*, vol. 13, no. 24, 2023, doi: 10.3390/app132413269.

[32] A. Alanazi and A. Gumaei, "A Decision-Fusion-Based Ensemble Approach for Malicious Websites Detection," *Appl. Sci.*, vol. 13, no. 18, 2023, doi: 10.3390/app131810260.

[33] A. A. Ajhari, D. F. Priambodo, R. H. Paradisa, and H. Yulianti, "PROCTOR: A Robust URL Protection System Against Fraudulent, Phishing, and Scam Activities," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 1013–1021, 2023, doi: 10.12785/IJCDS/140179.

[34] S. Abad, H. Gholamy, and M. Aslani, "Classification of Malicious URLs Using Machine Learning," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23187760.

[35] A. S. Rafsanjani, N. B. Kamaruddin, M. Behjati, S. Aslam, A. Sarfaraz, and A. Amphawan, "Enhancing Malicious URL Detection: A Novel Framework Leveraging Priority Coefficient and Feature Evaluation," *IEEE Access*, vol. 12, no. April, pp. 85001–85026, 2024, doi: 10.1109/ACCESS.2024.3412331.

[36] Z. Fan, W. Li, K. B. Laskey, and K. C. Chang, "Investigation of Phishing Susceptibility with Explainable Artificial Intelligence," *Futur. Internet*, vol. 16, no. 1, 2024, doi: 10.3390/fi16010031.

[37] M. W. Shaukat, R. Amin, M. M. A. Muslam, A. H. Alshehri, y J. Xie, "A Hybrid Approach for Alluring Ads Phishing Attack Detection Using Machine Learning," *Sensors*, vol. 23, no. 19, p. 8070, Sep. 2023. DOI: 10.3390/s23198070.

[38] K. Omari, "Comparative Study of Machine Learning Algorithms for Phishing Website Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 9, pp. 417–425, 2023, doi: 10.14569/IJACSA.2023.0140945.

[39] M. K. Prabakaran, P. Meenakshi Sundaram, and A. D. Chandrasekar, "An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders," *IET Inf. Secur.*, vol. 17, no. 3, pp. 423–440, 2023, doi: 10.1049/ise2.12106.

[40] M. A. Qasim and N. A. Flayh, "Enhancing Phishing Website Detection via Feature Selection in URL-Based Analysis," *Inform.*, vol. 47, no. 9, pp. 145–155, 2023, doi: 10.31449/inf.v47i9.5177.

[41] F. A. Demmese, S. Shajarian, and S. Khorsandroo, "Transfer learning with ResNet50 for malicious domains classification using image visualization," *Discov. Artif. Intell.*, vol. 4, no. 1, 2024, doi: 10.1007/s44163-024-00154-z.

[42] A. A. Tenis and R. Santhosh, "Modelling an Efficient URL Phishing Detection Approach Based on a Dense Network Model," *Comput. Syst. Sci. Eng.*, vol. 47, no. 2, pp. 2625–2641, 2023, doi: 10.32604/csse.2023.036626.

[43] M. A. Alsharaiah *et al.*, "A new phishing-website detection framework using ensemble classification and clustering," *Int. J. Data Netw. Sci.*, vol. 7, no. 2, pp. 857–864, 2023, doi: 10.5267/j.ijdns.2023.1.003.

[44] S. R. Abdul Samad *et al.*, "Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection," *Electron.*, vol. 12, no. 7, 2023, doi: 10.3390/electronics12071642.

[45] E. A. Aldakheel, M. Zakariah, G. A. Gashgari, F. A. Almarshad, and A. I. A. Alzahrani, "A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators," *Sensors*, vol. 23, no. 9, 2023, doi: 10.3390/s23094403.

[46] A. Ozcan, C. Catal, E. Donmez, and B. Senturk, "A hybrid DNN–LSTM model for detecting phishing URLs," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 4957–4973, 2023, doi: 10.1007/s00521-021-06401-z.

[47] R. Pal, M. K. Pandey, S. Pal, and D. C. Yadav, "Phishing Detection: A Hybrid Model with Feature Selection and Machine Learning Techniques," *Int. J. Exp. Res. Rev.*, vol. 36, pp. 99–108, 2023, doi: 10.52756/ijerr.2023.v36.009.

[48] L. Mat Rani, C. F. Mohd Foozy, and S. N. B. Mustafa, "Feature Selection to Enhance Phishing Website Detection Based On URL Using Machine Learning Techniques," *J. Soft Comput. Data Min.*, vol. 4, no. 1, pp. 30–41, 2023, doi: 10.30880/jscdm.2023.04.01.003.

[49] C. Zonyfar, J. B. Lee, and J. D. Kim, "HCNN-LSTM: Hybrid Convolutional Neural Network with Long Short-Term Memory Integrated for Legitimate Web Prediction," *J. Web Eng.*, vol. 22, no. 5, pp. 757–782, 2023, doi: 10.13052/jwe1540-9589.2251.

[50] H. Salah and H. Zuhair, "Deep learning in phishing mitigation: a uniform resource locator-based predictive model," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 3, pp. 3227–3243, 2023, doi: 10.11591/ijece.v13i3.pp3227-3243.

[51] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing Detection System Through Hybrid Machine Learning Based on URL," *IEEE Access*, vol. 11, no. January, pp. 36805–36822, 2023, doi: 10.1109/ACCESS.2023.3252366.

[52] L. R. Kalabarige, R. S. Rao, A. R. Pais, and L. A. Gabralla, "A Boosting-Based Hybrid Feature Selection and Multi-Layer Stacked Ensemble Learning Model to Detect Phishing Websites," *IEEE Access*, vol. 11, no. July, pp. 71180–71193, 2023, doi: 10.1109/ACCESS.2023.3293649.

[53] D. T. Mosa, M. Y. Shams, A. A. Abohany, E. S. M. El-Kenawy, and M. Thabet, "Machine Learning Techniques for Detecting Phishing URL Attacks," *Comput. Mater. Contin.*, vol. 75, no. 1, pp. 1271–1290, 2023, doi: 10.32604/cmc.2023.036422.

[54] A. H. Aljammal, S. taamneh, A. Qawasmeh, and H. B. Salameh, "Machine Learning Based Phishing Attacks Detection Using Multiple Datasets," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 5, pp. 71–83, 2023, doi: 10.3991/ijim.v17i05.37575.

[55] N. Innab *et al.*, "Phishing Attacks Detection Using EnsembleMachine Learning Algorithms," *Comput. Mater. Contin.*, vol. 80, no. 1, pp. 1325–1345, 2024, doi: 10.32604/cmc.2024.051778.