Polo del Conocimiento

Pol. Con. (Edición núm. 80) Vol. 8, No 3
Marzo 2023, pp. 2618-2634
ISSN: 2550 - 682X
DOI: 10.23857/pc.v8i3

Revisión de la literatura de las metodologías de ciberseguridad en plataformas bancarias

Review of the literature of cybersecurity methodologies in banking platforms

Revisão de literatura sobre metodologias de cibersegurança em plataformas bancárias

Francisco Xavier Morales-García I
fmorales5932@utm.edu.ec

Jorge Luis Zambrano-Martínez II
jorge.zambrano01@utm.edu.ec

Correspondencia: fmorales5932@utm.edu.ec

Ciencias Económicas y Empresariales.
Artículo de Investigación.

***Recibido:** 23 de enero de 2022 ***Aceptado:** 12 de febrero de 2022 *** Publicado:** 24 de marzo de 2022

I. Instituto de Posgrado, Universidad Técnica de Manabí, Ecuador.
II. Facultad de Ciencias Informáticas, Universidad Técnica de Manabí, Ecuador.

Resumen

Actualmente, la bancarización en línea es una herramienta fundamental para las personas naturales o jurídicas, llegando a que los servicios bancarios que se realizaban de manera tradicional (forma física), se trasladen hacia el internet debido por su facilidad de uso y comodidad para el cliente, teniendo estos servicios a su disposición en cualquier momento. Por este motivo, estos servicios bancarios en línea llegan a ser atractivo para delincuentes por lo que idean diversas estrategias para generar ataques a los centros de datos de las agencias bancarias, con la finalidad de obtener la mayor información posible de los usuarios y así sustraer de manera ilegal información y dinero de entidades bancarias. El presente trabajo investigativo tiene como objetivo realizar una revisión bibliográfica, utilizando la metodología de revisión sistemática de la literatura, SLR, seleccionando de manera exhaustiva y adecuada la información, a través de investigación de estudios relacionados a los algoritmos de seguridad informática necesarios para contrarrestar ataques de seguridad informática que son objetivos las plataformas de banca en línea para conocer la preparación y propuesta ante inconvenientes de seguridad que posee la banca en línea, utilizando variedad de investigaciones en publicaciones, revistas y otros elementos de investigación que permitirán desarrollar el presente artículo de revisión. Los resultados obtenidos permiten concluir que los algoritmos de seguridad basados en DHCP Snooping permiten ser el principio de varios puntos y propuestas para contrarrestar ataques a servidores de banca en línea de plataformas financieras. A través de DHCP Snooping, se permite contrarrestar al DHCP Spoofing que es el principio de la mayoría de ataques en línea a diferentes sistemas y aplicaciones de ciberseguridad. En cuanto a los trabajos implementados se identificaron diferentes alternativas para contrarestar ataques utilizando DHCP Snooping a través de sus múltiples ofrecimientos de soluciones para protección de servidores de banca en línea.

Palabras clave: Protección; Bancarización; Datos; Ciberseguridad; Digitalización.

Abstract

Currently, online banking is a fundamental tool for natural or legal persons, leading to the fact that banking services that were carried out in a traditional way (physical form), are transferred to the internet due to its ease of use and comfort for the client. , having these services at your disposal at any time. For this reason, these online banking services become attractive to criminals, which is why they devise various strategies to generate attacks on the data centers of banking agencies, in

order to obtain as much information as possible from users and thus steal from information and money from banking entities illegally. The objective of this investigative work is to carry out a bibliographic review, using the methodology of systematic review of the literature, SLR, selecting the information in an exhaustive and adequate way, through research of studies related to the computer security algorithms necessary to counterattacks. of computer security that online banking platforms are objectives to know the preparation and proposal for security problems that online banking has, using a variety of research in publications, magazines and other research elements that will allow the development of this review article . The results obtained allow us to conclude that the security algorithms based on DHCP Snooping can be the beginning of various points and proposals to counteract attacks on online banking servers of financial platforms. Through DHCP Snooping, it is possible to counteract DHCP Spoofing, which is the principle of most online attacks on different cybersecurity systems and applications. As for the work implemented, different alternatives were identified to counter attacks using DHCP Snooping through its multiple offerings of solutions for the protection of online banking servers.

Keywords: Protection; banking; Data; cybersecurity; Digitization.

Resumo

Atualmente, a banca online é uma ferramenta fundamental para as pessoas singulares ou coletivas, levando a que os serviços bancários que eram efetuados de forma tradicional (forma física), sejam transferidos para a internet devido à sua facilidade de utilização e conforto para o cliente . , tendo estes serviços à sua disposição a qualquer momento. Por esse motivo, esses serviços bancários online tornam-se atraentes para os criminosos, por isso eles criam várias estratégias para gerar ataques aos data centers das agências bancárias, a fim de obter o máximo de informações possíveis dos usuários e, assim, roubar informações e dinheiro de entidades bancárias ilegalmente. O objetivo deste trabalho investigativo é realizar uma revisão bibliográfica, utilizando a metodologia de revisão sistemática da literatura, SLR, selecionando as informações de forma exaustiva e adequada, por meio de pesquisa de estudos relacionados aos algoritmos de segurança de computadores necessários para contra-ataques. de segurança informática que as plataformas de banca online têm como objetivos conhecer a preparação e proposta de problemas de segurança que a banca online apresenta, recorrendo a diversas pesquisas em publicações, revistas e outros elementos de pesquisa que permitirão o desenvolvimento deste artigo de revisão. Os resultados obtidos permitem concluir

que os algoritmos de segurança baseados em DHCP Snooping podem ser o início de vários pontos e propostas para contrariar ataques a servidores de banca online de plataformas financeiras. Por meio do DHCP Snooping, é possível neutralizar o DHCP Spoofing, que é o princípio da maioria dos ataques online a diferentes sistemas e aplicativos de segurança cibernética. Quanto ao trabalho implementado, foram identificadas diferentes alternativas para combater os ataques utilizando DHCP Snooping através das suas múltiplas ofertas de soluções para a proteção de servidores de banca online.

Palavras-chave: Proteção; bancário; Dados; cíber segurança; Digitalização.

Introducción

En la actualidad, resulta sumamente sencillo crear y compartir información con la idea de simplificar la vida de manera general a los usuarios a través de plataformas en línea. Un ejemplo claro son las páginas web y las aplicaciones bancarias, en donde la unión de estos servicios permite una integración donde facilita las actividades bancarias a personas y compañías a través de servicios de internet. Es fundamental tener en cuenta el diseño e implementación de objetivos estratégicos y operacionales dentro del sector bancario para una mayor competitividad, y sobre todo generar confianza en la clientela de una entidad bancaria. La vulneración a servicios donde concentra cantidades de dinero considerables no es solo el objetivo principal de los ataques informáticos, que es una de las motivaciones que tienen los atacantes al momento de vulnerar una entidad bancaria. Otro motivo en el por qué los atacantes vulneran los servicios bancarios en línea, es la información personal de los clientes y administradores, que son de los servidores y equipos del sistema bancario al no poseer su respectiva seguridad mediante dispositivos físicos o lógicos, denegación de servicios en línea, eliminación de reglas de seguridad configuradas en los cortafuegos (firewall) y la extracción de información confidencial. Estas son algunas formas que generan inestabilidad en los modelos de seguridad informática y que son utilizados y atacados por ciberdelincuentes, quienes desarrollan software malicioso (malware) para infiltrarse y causar daño al sistema. Estas vulnerabilidades creadas permiten obtener información para fines lucrativos e ilegales, en donde los atacantes buscan un beneficio personal.

Según Llamuca Pérez (Llamuca-Pérez, 2019), Ecuador actualmente es común observar a los clientes en las entidades bancarias haciendo largas filas para realizar transferencias bancarias, ya sean depósitos, retiros, cobros de cheques, pago de planillas, entre otros servicios; ocasionando

insatisfacción y molestia a los clientes o usuarios, a pesar que en los últimos años han realizado enormes esfuerzos por parte del sector bancario para mejorar los niveles de satisfacción de los clientes al modernizar la banca ecuatoriana con la creación de la banca virtual o e-banking.

Sin embargo, acorde a lo mencionado por Ochoa (2021), por medio de ingeniería social se realizan ataques cibernéticos, que crean afectaciones a usuarios y servidores, en donde la falta de seguridad institucional, en este caso de estudio, la seguridad informática de servidores financieros, influya en la necesidad de tener mejores mecanismos ante estos ataques, logrando así, obtener un nivel adecuado de ciberseguridad, donde se logre establecer una prevención de ataques a servidores a través de algoritmos de ciberseguridad, para este caso, las plataformas de bancas en línea de entidades financieras.

El presente trabajo tiene como objetivo realizar una revisión bibliográfica de los estudios realizados algoritmos que permiten alterar la seguridad a sistemas de banca en línea de entidades financieras, así como de algoritmos para protección de datos en los servidores de las plataformas mencionadas, con el fin de lograr obtener una perspectiva más acertada de las principales vulnerabilidades y sus potenciales soluciones ante los inconvenientes de ataques a las plataformas de banca en línea.

Metodologia

La presente investigación es de tipo documental, donde se empleó una revisión bibliográfica a los trabajos referentes a tópicos relacionados con seguridad informática, banca en línea y temas relacionados a vulnerabilidades de servidores y aplicaciones en línea que existen en la banca en línea. Se realizaron búsquedas de artículos científicos, publicaciones de revista, conferencias internacionales y tesis de posgrado obtenidas principalmente de bases bibliográficas de la IEEE Xplorer, Science Direct, Web of Science, ResearchGate y repositorios institucionales. En un periodo de búsqueda de publicaciones desde el año 2017 hasta la actualidad, donde la tendencia sobre la seguridad informática de banca en línea creció de manera exponencial. Las cadenas de búsqueda empleadas en esta investigación para encontrar de manera resumida los trabajos son las siguientes: ¨All Metadata":cybersecurity AND All Metadata":e-banking” y All Metadata":data protection "All Metadata":banking”, Con lo cual se logró reducir de manera muy precisa la cantidad de trabajos para la posterior revisión y análisis de la información de los sistemas para la valoración de los procesos, equipos o tecnologías entre las más adecuada e idónea en la

Pol. Con. (Edición núm. 80) Vol. 8, No 3 Marzo 2023, pp. 2618-2634, ISSN: 2550 - 682X

implementación de metodología de seguridad informática para protección de plataformas de banca en línea.

Posteriormente se los trabajos de acuerdo con el enfoque de las investigaciones, obteniendo la siguiente clasificación:

- Investigaciones y propuestas de algoritmos y seguridad informática para protección de sistemas, servidores y aplicaciones de banca en línea.
- Implementación de sistemas y algoritmos de seguridad informática.
- Estudios de vulnerabilidades y algoritmos de protección ante ataques.

Así mismo, se realizó un análisis descriptivo de los estudios encontrados en cada criterio de clasificación considerado.

Resultados

Una vez realizada la búsqueda se obtuvieron 21 artículos desde el año 2017 hasta la actualidad. Los estudios presentados a continuación son el resultado de la ejecución de los procedimientos declarados en la presente investigación.

En la Figura 1 se presentan el número de estudios encontrados desde el año 2017 hasta el 2021.

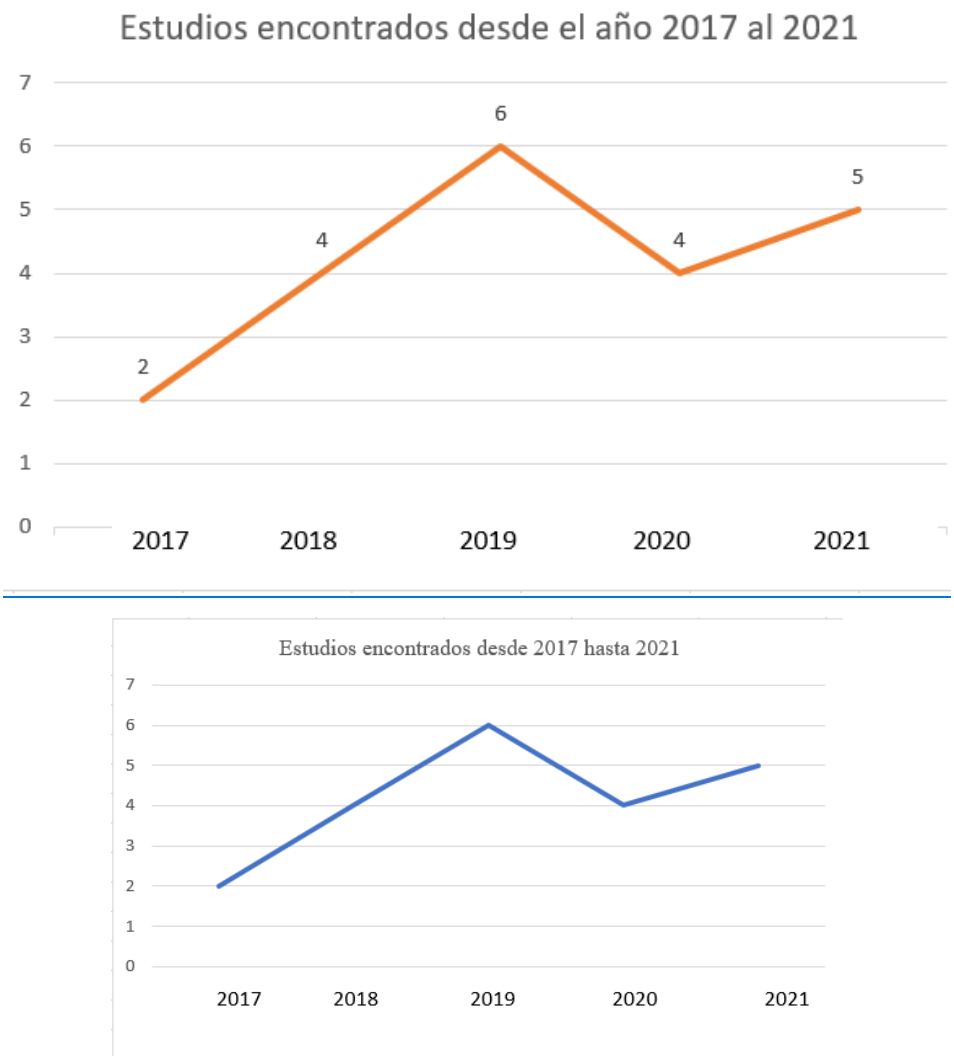
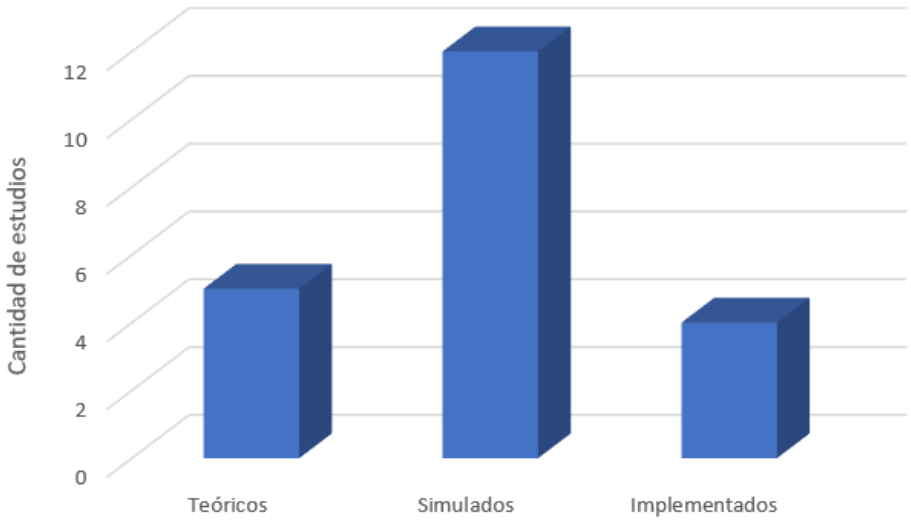


Figura 1. Número de estudios encontrados desde el año 2017 hasta el 2021

Se observa que desde el año 2017 se obtuvo un crecimiento de trabajo hasta el año 2019 se tuvo gran cantidad de documentación e investigaciones, siendo el año 2020 el momento donde los elementos a estudiar bajaron considerablemente y en el año 2021 subió un considerable más de artículos de estudio.

A continuación, en la Figura 2 se presenta la cantidad de estudios que se encontraron de acuerdo con la clasificación mencionada en la sección de materiales y métodos.

Pol. Con. (Edición núm. 80) Vol. 8, No 3 Marzo 2023, pp. 2618-2634, ISSN: 2550 - 682X



	Cantidad de estudios
Teóricos	5
Simulados	12
Implementados	4

Figura 2. Número de estudios encontrados desde el año 2017 hasta el 2021

En la figura 2 se logra apreciar que la temática con mayor cantidad de trabajos encontrados son los de tipo implementados o investigaciones de propuestas. ~~Teniendo en menor cantidad los trabajos con implementaciones.~~ Teniendo en menor cantidad los trabajos con implementaciones. El motivo al cual se encuentran más trabajos teóricos o implementados se debe a que la simulación y trabajos teóricos tienen un costo muy accesible para ser realizado sin ningún inconveniente.

Investigaciones y noticias sobre la seguridad informática para la banca en línea

Los trabajos en este criterio se enfocaron en realizar investigaciones para temas de seguridad informática, enmarcados y destinados a la protección de datos en los sistemas de banca en línea, tanto para cuidado de datos y de contenido financiero.

Según la definición de Bhosale (2018), el término ciberseguridad es usado a nivel global que crean servicios a través de internet donde se requiera trabajar en la protección ante ataques y vulnerabilidad de los sistemas que ofrecen estos servicios de manera global.

Bilge (2019) explica que, los ataques más comunes que se deben tener en cuenta en sistemas de seguridad informática, para este caso de investigación, la banca en línea son: Phishing, Keylogger, Ingeniería social, ataque de fuerza bruta y spam, ya que estos ataques mencionados son comunes para la obtención de manera ilegal de información y contenido financiero presente en las plataformas de banca en línea, considerado uno de los puntos más vulnerados en internet por la calidad de información que existen en estos sistemas.

Tok (2021) explica en sus definiciones que, para poder proyectar estos ataques se utiliza el algoritmo de DHCP Spoofing, por el cual permite enviar ataques a través de los servidores y sistemas por medio de los protocolos de red como el protocolo de resolución de dirección, por sus siglas en inglés ARP, usando técnicas a través del protocolo de acceso de control de multimedia, por su siglas en ingles MAC, usando el protocolo de internet IP y por medio de las DNS. EL DHCP Spoofing permite crear estos algoritmos para crear ataques mencionados en el párrafo anterior y así poder vulnerar información de sistemas de seguridad informática.

Ojeda-Contreras (2020) ha explicado en artículos basados en noticias de manera global que, a medida en que las instituciones financieras implementen nuevos servicios y operaciones digitales, estas se convierten en blanco de mayores riesgos de ataques cibernéticos, que pueden suceder y por ende ver vulnerada su seguridad e información almacenada en sus equipos. La digitalización de servicios bancarios por parte de las entidades financieras debe responder a los cambios del nuevo entorno competitivo y de los hábitos de los consumidores, por tanto, así como de la protección de datos que conlleva a un trabajo más sofisticado para evitar ataques que comprometan la seguridad de la banca en línea.

Kwom (2018) explica detalles sobre los ecosistemas de PKI de firma de código son vulnerables a los abusadores. Kim et al. informó tales casos de abuso, *por ejemplo,* los autores de malware hicieron un mal uso de las claves privadas robadas de los certificados de firma de código acreditados para firmar sus programas maliciosos. esta certificado el malware explota la cadena de

Pol. Con. (Edición núm. 80) Vol. 8, No 3 Marzo 2023, pp. 2618-2634, ISSN: 2550 - 682X

confianza establecida en el ecosistema y ayuda a un adversario a eludir fácilmente los mecanismos de seguridad, con lo que se debe trabajar para evitar problemas que comprometan información en banca en línea.

Burris (2018) explica que parte de los desafíos para mantener la seguridad dentro de una organización es la capacitación de una fuerza laboral no técnica para responder adecuadamente a las amenazas de seguridad cibernética. El Desarrollo de un entorno en línea que utiliza el aprendizaje experiencial para brindar a los trabajadores no técnicos una mayor exposición a los problemas de ciberseguridad.es importante a través de un enfoque basado en simulación que proporciona una mejor comprensión de las amenazas específicas de ciberseguridad a través del aprendizaje experiencial.

Alqahtani (2018) explica que, en la rama de la ciberseguridad, el comportamiento humano es considerado como el eslabón más débil. Es por ende que la capacitación de los usuarios sobre el tema de la ciberseguridad es importante para evitar ataques a su información, ya que el conocimiento de normas y protocolos, permite evitar inconvenientes a futuro para muchos usuarios y por ende a servidores y administradores.

En complemento a las investigaciones revisadas se presenta un resumen de estos, como se aprecia en la Tabla 3

Tabla 3. Resumen de los estudios de investigaciones y propuestas de algoritmos para seguridad en plataformas en línea

Referencia	Tema de investigación
(Bilge, 2019),	An Empirical Study of Zero-Day Attacks In The Real World
(Alqahtani, 2018)	Does Decision-Making Style Predict Individuals' Cybersecurity Avoidance Behaviour?
(Brosalle, 2018)	Research Paper on Cyber Security

(Burris, 2018)	Activity Simulation for Experiential Learning in Cybersecurity Workforce Development
(Kwom, 2018)	Certified Malware in South Korea: A Localized Study of Breaches of Trust in Code-Signing PKI Ecosystem
(Ojeda-Contreras, 2020)	Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador
(Tok, 2021)	Security analysis of SDN controller-based DHCP services and attack mitigation with DHCP guard

Implementación de algoritmos de seguridad para protección de datos y políticas

Los trabajos en este criterio se enfocaron en realizar investigaciones a nivel de implementación, simulación y prototipos experimentales, se incluyen aquellos que se plantean para crear algoritmos de seguridad informática para plataformas financieras de banca en línea. En la Tabla 4 mostrada se describe los trabajos de implementación, con algoritmos para protección de banca en línea.

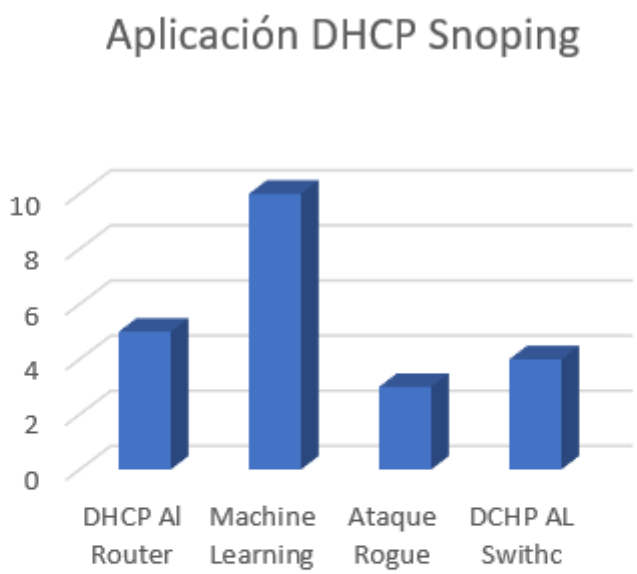
Tabla 4. Descripción de algoritmos utilizados para protección de datos en plataformas de banca en línea

Referencia	**Algoritmos utilizados.**
(Adjei, 2021)	Inspección de DHCP Snooping y ARP Spoofing
(Toorn, 2021)	Desafíos DNS A través de DHCP Snooping
(Akashi, 2019)	A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping: To what extent can DHCP snooping protect clients from the cyberattack based on DHCP spoofing
(Syed, 2021)	Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks
(Delija, 2021)	An Analysis of Wireless Network Security Test Results provided by Raspberry Pi Devices on Kali Linux

(Yardley, 2020)	CCNP Studies: Configuring DHCP Snooping
(Jevitha, 2017)	PAC File Based Attack con DHCP Snooping
(Tripathi, 2018)	Detecting stealth DHCP starvation attack using machine learning approach
(Aldaoud, 2021)	DHCP attacking tools: an analysis
(Nikolchev, 2020)	Development of Recommendations for the Implementation of Integrated Security in the Corporate Network at the OSI Data Link Layer
(Budiman, 2021)	The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack
(Ravishankar, 2021)	DHCP Origin Traceback
(Chapman, 2018)	DHCP Network elements and algorithms
(Dixit, 2021)	**Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review**

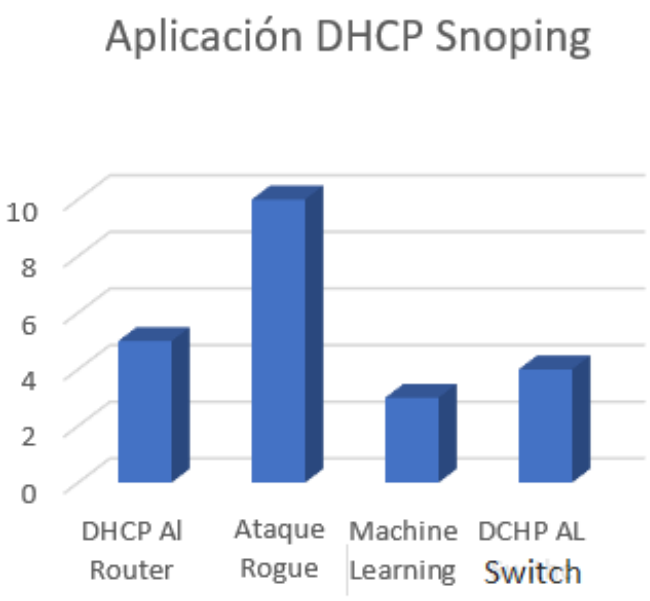
Como se puede observar en la Tabla 4, las simulaciones están dadas con DHCP Snoopíng, la tecnología y algoritmo más utilizado para prevención de ataques. Cabe recalcar que con base a todas las investigaciones creadas de este algoritmo se determinan varias decisiones y otros elementos claves para la prevención de ataques de seguridad informática, aplicados de manera general y a todos los sistemas que necesiten de implementar ciberseguridad. Para este caso se estudia a las plataformas de banca en línea.

A continuación, en la Figura 3 se presenta una comparación de los tipos de algoritmos DHCP Snooping para prevención de ataques.



	Aplicación DHCP Snoping
DHCP Al Router	5
Machine Learning	10
Ataque Rogue	3
DCHP AL Swithc	4

Pol. Con. (Edición núm. 80) Vol. 8, No 3 Marzo 2023, pp. 2618-2634, ISSN: 2550 - 682X



	Aplicación DHCP Snoping
DHCP Al Router	10
Machine Learning	5
Ataque Rogue	3
DHCP Al Switch	4

. **Figura 34.** Comparación de los algoritmos mencionados con mayor frecuencia en los trabajos

Conclusión

Se concluye que, al realizarlas revisiones necesarias para la literatura del presente proyecto, se concluye que con base a la investigación dada se obtuvieron datos con base a estadísticas filtradas para proyectos de investigación para seguridad informática en plataformas financieras. Con porcentajes dados de trabajo en temas de recolectar artículos filtrados sobre ciberseguridad y bancarización, dividido en porcentajes de artículos adecuados de información filtrada de un 23.80% de datos distribuido en tres buscadores y 14.28% para dos buscadores, permitió obtener datos a la vanguardia de las estadísticas que se necesitan para investigaciones acorde a los temas de Ciberseguridad, Bancarización, Protección de datos, Digitalización. Cabe recordar que, con base a todos estos datos adecuados, permitirá realizar trabajos futuros de investigación para trabajos de

ciberseguridad. Si bien esta investigación se enfoca a través de la seguridad informática en bancarización en línea, permite tener datos para trabajos futuros en investigaciones acordes a los temas Seguridad para correos electrónicos, seguridad en temas de sistema de administración de contenidos. seguridad en pasarelas de pago seguridad en sistemas de gestión de aplicaciones gubernamentales.

Con base a esta investigación, los trabajos futuros mencionados pueden basarse en esta investigación para enfocarse en temas parecidos. La única diferencia con este trabajo será el tema de enfoque para cualquier investigación dada sobre temas de seguridad informática o ciberseguridad.

Referencia

1. Aldaoud, M., Al-Abri, D., Al Maashri, A. et al. DHCP attacking tools: an analysis. J Comput Virol Hack Tech 17, 119–129 (2021). https://doi.org/10.1007/s11416-020-00374-8
2. Alqahtani, H., Kavakli-Thorne, M. (2020). Does Decision-Making Style Predict Individuals' Cybersecurity Avoidance Behaviour?. In: Moallem, A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2020. Lecture Notes in Computer Science(), vol 12210. Springer, Cham. https://doi.org/10.1007/978-3-030-50309-3_3
3. Bhosale, Sachin & Sharma, Yogeshkumar & Karekar, Miss & Jagdishprasad, Shri & Tibrewala, Jhabarmal. (2021). Machine Learning in Bioinformatics. 2021. https://www.researchgate.net/publication/352477760_Machine_Learning_in_Bioinformatics
4. Bilge, L. (2019). http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf
5. Brocen, J. (2018). Guidelines for designing e-statements for e-banking https://dl.acm.org/doi/10.1145/3283458.3283461,
6. Brosens, J. (2018). https://dl.acm.org/doi/10.1145/3283458.3283461
7. Burris, J., Deneke, W., Maulding, B. (2018). Activity Simulation for Experiential Learning in Cybersecurity Workforce Development. In: Nah, FH., Xiao, B. (eds) HCI in Business, Government, and Organizations. HCIBGO 2018. Lecture Notes in Computer Science(), vol 10923. Springer, Cham. https://doi.org/10.1007/978-3-319-91716-0_2
8. Chapman, C. (2017). ScienceDirect. https://www.sciencedirect.com/science/article/pii/B9780128035849000111

9. D. Delija, Ž. Petrović, G. Sirovatka and M. Žagar, "An Analysis of Wireless Network Security Test Results provided by Raspberry Pi Devices on Kali Linux," 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2021, pp. 1219-1223, : doi: https://www.researchgate.net/profile/Damir-Delija/publication/356240379_An_Analysis_of_Wireless_Network_Security_Test_Results_provided_by_Raspberry_Pi_Devices_on_Kali_Linux/links/61e831278d338833e37dff34/An-Analysis-of-Wireless-Network-Security-Test-Results-provided-by-Raspberry-Pi-Devices-on-Kali-Linux.pdf
10. Dixit, P. (2021). Science Direct. https://www.sciencedirect.com/science/article/abs/pii/S1574013720304172
11. G. Ninahualpa, S. Yoo, T. Guarda, J. Díaz and D. Piccirilli, "Protocol of Information Recovery in Solid Hard Drives - SSD Using File Carving Techniques," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-6, doi: 10.23919/CISTI.2019.8760783.
12. Henríquez, E. &. (2013). . Preparación de un proyecto de investigacion. Henríquez, E., &Zepeda, M. (2003).
13. Jacques Brosens, Rendani M. Kruger, and Hanlie Smuts. (2018). Guidelines for designing e-statements for e-banking. In Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities (AfriCHI '18). Association for Computing Machinery, New York, NY, USA, Article 13, 1–6.
14. K. Nikolchev, K. Herasymenko, O. Starkova and M. Yastrebov, "Development of Recommendations for the Implementation of Integrated Security in the Corporate Network at the OSI Data Link Layer," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 807-810, : doi: 10.1109/PICST51311.2020.9468014.
15. Kwon, B., Hong, S., Jeon, Y., Kim, D. (2021). Certified Malware in South Korea: A Localized Study of Breaches of Trust in Code-Signing PKI Ecosystem. In: Gao, D., Li, Q., Guan, X., Liao, X. (eds) Information and Communications Security. ICICS 2021. Lecture Notes in Computer Science(), vol 12918. Springer, Cham. https://doi.org/10.1007/978-3-030-86890-1_4

16. M. S. Abdullah, A. Zainal, M. A. Maarof and M. Nizam Kassim, "Cyber-Attack Features for Detecting Cyber Threat Incidents from Online News," 2018 Cyber Resilience Conference (CRC), 2018, pp. 1-4, doi: 10.1109/CR.2018.8626866.
17. Majumdar, S., Kulkarni, D., Ravishankar, C.V. (2011). DHCP Origin Traceback. In: Aguilera, M.K., Yu, H., Vaidya, N.H., Srinivasan, V., Choudhury, R.R. (eds) Distributed Computing and Networking. ICDCN 2011. Lecture Notes in Computer Science, vol 6522. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-17679-1_35
18. Mantenola, C. (2009).Revisión sistemática de la Literatura. Obtenido de https://www.elsevier.es/es-revista-cirugia-espanola-36-articulo- revisiones-sistematicas-literatura-que-se-S0009739X11003307. Página 25
19. Ojeda-Contreras, F. I. (2020).. Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuado https://dialnet.unirioja.es/descarga/articulo/8316317.pdf
20. Pradana, Dio & Budiman, Ade. (2021). The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. IJID (International Journal on Informatics for Development). 10. 38-46. 10.14421/ijid.2021.2287.
21. S. Syed, F. Khuhawar, S. Talpur, A. A. Memon, M. -A. Luque-Nieto and S. Narejo, "Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks," 2022 Global Conference on Wireless and Optical Technologies (GCWOT), Malaga, Spain, 2022, pp. 1-7, doi: 10.1109/GCWOT53057.2022.9772887
22. S. Syed, F. Khuhawar, S. Talpur, A. A. Memon, M. -A. Luque-Nieto and S. Narejo, "Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks," 2022 Global Conference on Wireless and Optical Technologies (GCWOT), Malaga, Spain, 2022, pp. 1-7, doi: 10.1109/GCWOT53057.2022.9772887.
23. Sanchez, E. B. (2003).Obtenido de https://www.postgradoune.edu.pe/pdf/documentos-academicos/ciencias-de-la-educacion/13.pdf
24. Tok, M. S. (2021). Science direct. (Tok, ScienceDirect, 2021)Tripathi, N. (2018). Springer. https://link.springer.com/article/10.1007/s11416-017-0310-x
25. Tok, M. S. (2021). ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0167404821002182

26. Tong, Yao & Akashi, Shigeo. (2019). A Feasible Method for Realizing Leakage of DHCP Transactions under the Implementation of DHCP Snooping: To what extent can DHCP snooping protect clients from the cyberattack based on DHCP spoofing. DSIT 2019: Proceedings of the 2019 2nd International Conference on Data Science and Information Technology. https://dl.acm.org/doi/abs/10.1145/3352411.3356103
27. Toorn, O. v. (2022). ScienceDirect. https://www.sciencedirect.com/science/article/pii/S1574013722000132
28. Yardley, E. (2020). CCNP Studies: Configuring DHCP Snooping https://packetpushers.net/ccnp-studies-configuring-dhcp-snooping/