https://doi.org/10.56469/rcti.v22i32.967

La importancia de la auditoría de seguridad en redes informáticas

The importance of security auditing in computer networks

Maricielo Estefany Caciano Arroyo [1]✉ • Antony Fernando Vasquez Cabrera [1] • Alberto Carlos Mendoza de los Santos [1]

Recibido: 6 Marzo 2024 / Revisado: 26 Abril 2024 / Aceptado: 7 Julio 2024 / Publicado: 14 Noviembre 2024

Resumen

La seguridad de la red es fundamental para salvaguardar los datos y mantener la permanencia de las operaciones. La auditoría de seguridad de la red desempeña un papel crucial al evaluar y mejorar los controles, identificando riesgos y garantizando el cumplimiento de los estándares de control. El propósito de la investigación fue establecer la importancia de la auditoría en la protección de las redes dentro de un contexto cada vez más digital. Mediante la aplicación de la metodología PRISMA, se llevó a cabo una evaluación meticulosa de publicaciones científicas, filtrando los artículos por año, título y principales aportes, proporcionando un análisis más detallado. Los resultados revelaron el impacto significativo de la auditoría en la seguridad de la red en diversas áreas tecnológicas de una organización. Se destacó que la efectividad de la auditoría de seguridad de red aumenta con el progreso en la gestión del riesgo, y se resaltó el valor de herramientas como Nmap y técnicas de minería de datos para analizar y fortalecer la seguridad de las redes. En conclusión, la auditoría de seguridad de la red es indispensable para la protección de sistemas informáticos, el fortalecimiento de la ciberseguridad y la prevención de pérdidas de datos.

Palabras claves: Ciberseguridad, Vulnerabilidad, Internet, Infraestructura

Abstract

Network security is critical to safeguarding data and maintaining the permanence of operations. The audit of this process is crucial in assessing and improving controls, identifying risks, and ensuring compliance with control standards. The research aimed to establish the importance of auditing in protecting networks within an increasingly digital context. By applying the PRISMA methodology, scientific publications were meticulously

Antony Fernando Vasquez Cabrera
https://orcid.org/0009-0001-3151-2936

Alberto Carlos Mendoza de los Santos
https://orcid.org/0000-0002-0469-915X

✉ Maricielo Estefany Caciano Arroyo / t513300120@unitru.edu.pe
https://orcid.org/0009-0007-3444-7985

1 Universidad Nacional de Trujillo. Trujillo, Perú.

evaluated, and articles were filtered by year, title, and main contributions, providing a more detailed analysis. The results revealed the significant impact of auditing on network security in various technological areas of an organization. It also highlighted that the effectiveness of network security auditing increases with progress in risk management. The study emphasized using tools like Nmap and data mining techniques to analyze and strengthen network security. In conclusion, network security auditing is indispensable for protecting computer systems, strengthening cybersecurity, and preventing data loss.

Keywords: Cybersecurity, Vulnerability, Internet, Infrastructure.

Introducción

Una red es un conjunto de dispositivos tecnológicos que se comunican entre sí mediante protocolos y tecnologías cableadas o inalámbricas (AWS, 2023). Para salvaguardar la información y los recursos compartidos en la red, se requiere la implementación de medidas de seguridad en la infraestructura de la misma.

Preservar la seguridad de la red es fundamental para resguardar los datos y asegurar la continuidad de las operaciones de las organizaciones. Según Wang et al. (2022) la seguridad de la red consiste en aplicar medidas, técnicas y herramientas para proteger los datos, los sistemas y los dispositivos conectados a una red informática transparente y separada del servicio y el portador. Además, Tsao et al. (2022), incluye aspectos como la confidencialidad, la integridad, la disponibilidad, la autenticación y el no repudio de la información en la red. Por último, Morán y Maria (2021) indican que también implica prevenir, detectar y responder a las amenazas y los ataques que pueden afectar la seguridad de la red y sus componentes.

La seguridad de la red es un factor clave para el éxito y competitividad de las organizaciones, donde la información es un activo estratégico y la red es el medio principal para acceder a ella. De acuerdo con ASOBANCARIA (2022), la seguridad de la red permite compartir y procesar la información que permite asegurar la continuidad de las operaciones, la confianza de los clientes y los socios, el cumplimiento de las normativas y la reputación de la organización. Por el contrario, la falta de seguridad de la red puede ocasionar graves consecuencias, como la pérdida o el robo de datos, la interrupción o la degradación de los servicios, el daño a la imagen y la credibilidad, o la exposición a sanciones legales y financieras.

La protección de la red es un proceso dinámico que necesita una evaluación y mejora constante para enfrentar las amenazas y vulnerabilidades del entorno digital. Según Barclay Simpson (2022) esto implica realizar auditorías informáticas, que son un tipo de auditorías que usan las Tecnologías de Información (TI). La auditoría de seguridad de la red, de acuerdo con Najib et al. (2023), menciona que es una herramienta para comprobar el estado y la eficacia de los sistemas y controles que resguardan la información y los activos de la red.

Conforme a Morales et al. (2021), una auditoría de red efectiva conlleva un proceso estructurado que define el alcance y los objetivos planifica las actividades, recursos y responsabilidades, recopila información sobre la red y su entorno usando técnicas establecidas por organizaciones reconocidas en el campo de la seguridad informática, como SANS Institute, entre otras instituciones especializadas. Además, Koza (2022), analiza la evaluación de los controles de seguridad físicos y lógicos, basándose en normas y estándares internacionales como los establecidos por la ISO y el NIST. Este análisis también incluye una evaluación de riesgos que permite identificar, priorizar y mitigar los riesgos de seguridad existentes.

La auditoría de seguridad de la red tiene diversos y significativos beneficios. Según Canadian Centre for Cyber Security (2022), permite mejorar y

verificar las políticas y prácticas organizativas, evaluar las políticas y procesos según los estándares regulatorios y de cumplimiento, analizar la salud general de la infraestructura de red, descubrir e identificar ineficiencias, problemas, debilidades, vulnerabilidades y errores en la red.

Esta revisión sistemática busca explorar la relevancia de la auditoría en la seguridad de la red en el contexto actual de la protección de la información. La pregunta de investigación es: ¿Qué importancia tiene la auditoría en la seguridad de la red? Para responderla, se realizó una búsqueda exhaustiva en las principales fuentes académicas con temas relacionados la seguridad de la red y la auditoría informática. Se emplearon los criterios PRISMA para seleccionar y analizar los estudios relevantes encontrados, limitando el análisis al periodo entre el año 2021 y 2024.

Metodología

Antes de comenzar con la justificación de la metodología utilizada, es importante definir qué implica una revisión sistemática. Hoy en día, como señala Tapia-Benavente, et al. (2021) se considera que las revisiones sistemáticas son la mejor opción para apoyar decisiones bien fundamentadas debido a su capacidad para resumir la evidencia científica relevante sobre un tema, utilizando estándares metodológicos rigurosos en su evaluación. Este estudio se basa en un análisis minucioso y estructurado, gracias a la metodología PRISMA.

Según Barquero (2022), combina elementos conceptuales y metodológicos de las revisiones sistemáticas más recientes.

Para Ciapponi (2021), PRISMA 2020 se distinguen tres conceptos clave: el reporte, que es un documento detallado de un estudio; el registro, que consiste en el título de un reporte indexado en una base de datos; y el estudio, que es una investigación con participantes, intervenciones y resultados definidos, pudiendo generar varios reportes.

El proceso incluye la búsqueda de literatura, selección de investigaciones, revisión detallada, análisis y finalmente la síntesis de resultados. Se sigue la metodología PRISMA, que utiliza un protocolo predefinido, criterios de inclusión y exclusión, herramientas de evaluación crítica, recopilación de datos relevantes, y la presentación de diagramas de flujo y tablas resumen.

Estrategia de búsqueda

Se utilizaron términos clave extraídos de una búsqueda avanzada en la fuente de datos de SCOPUS, analizando 215 artículos, como método para recopilar la información relevante sobre el tema de investigación: TITLE-ABS-KEY (network AND security AND audit) AND PUBYEAR > 2020 AND PUBYEAR < 2025 AND (LIMIT-TO (EXACTKEYWORD , "Security Of Data") OR LIMIT-TO (EXACTKEYWORD,"Network Security") OR LIMIT-TO (EXACTKEYWORD , "Intrusion Detection") OR LIMIT-TO (EXACTKEYWORD ,"Security") OR LIMIT-TO (EXACTKEYWORD ,"Audit") OR LIMIT-TO (EXACTKEYWORD ,"Computer Networks")) AND (LIMIT-TO (SUBJAREA,"COMP") OR LIMIT-TO (SUBJAREA,"ENGI") OR EXCLUDE (SUBJAREA,"MEDI") OR EXCLUDE (SUBJAREA,"BIOC")) para posteriormente analizarlo en el software de análisis bibliográfico vosViewer y obtener palabras claves para la exploración en distintas fuentes de datos tal y como se muestra en la Figura 1.

Criterios de inclusión y exclusión

En lo que respecta a la elección de los documentos para el estudio, se examinaron investigaciones escritas en inglés utilizando diversas fuentes de datos para garantizar una muestra representativa. Se limitó la búsqueda a documentos publicados entre el 2021 y 2024 para asegurar la relevancia actualizada para la investigación en curso.

Además, se definieron categorías de documentos académicos para su inclusión, como artículos, presentaciones de conferencias y revisiones, siempre y cuando estuvieran disponibles en línea.

Por otro lado, se excluyeron publicaciones no relacionadas con la investigación, como los temas de medicina y salud, para asegurar que la selección de documentos estuviera alineada con los objetivos de la investigación, lo que contribuirá a mejorar la calidad y credibilidad de los resultados obtenidos tal y como se muestra en la Figura 2.

Figura 1. Análisis Bibliográfico

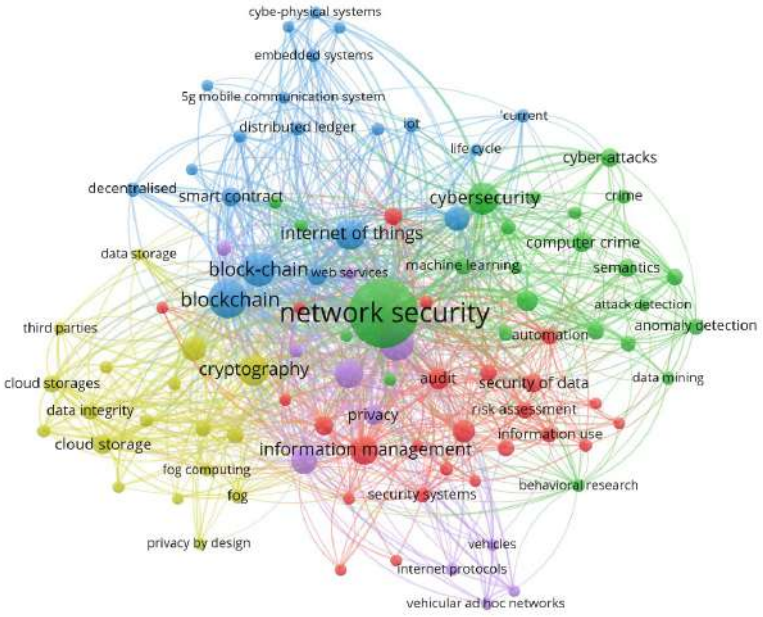
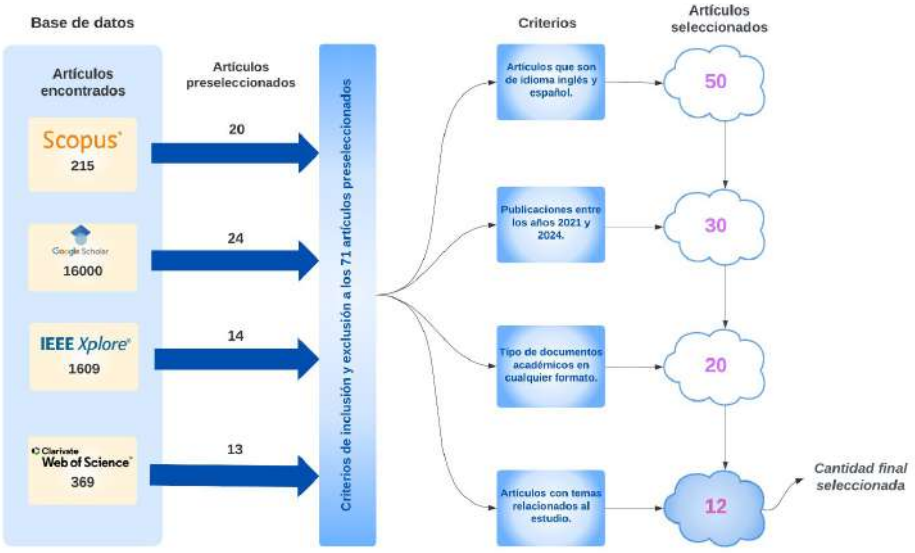


Figura 2. Criterios de exclusión e inclusión de los artículos encontrados en las bases de datos.



Resultados

En la Tabla 1 se muestra los resultados de la selección donde cada artículo satisfizo los criterios mencionados, proporcionando un análisis detallado de la importancia de la auditoria en la seguridad de la red.

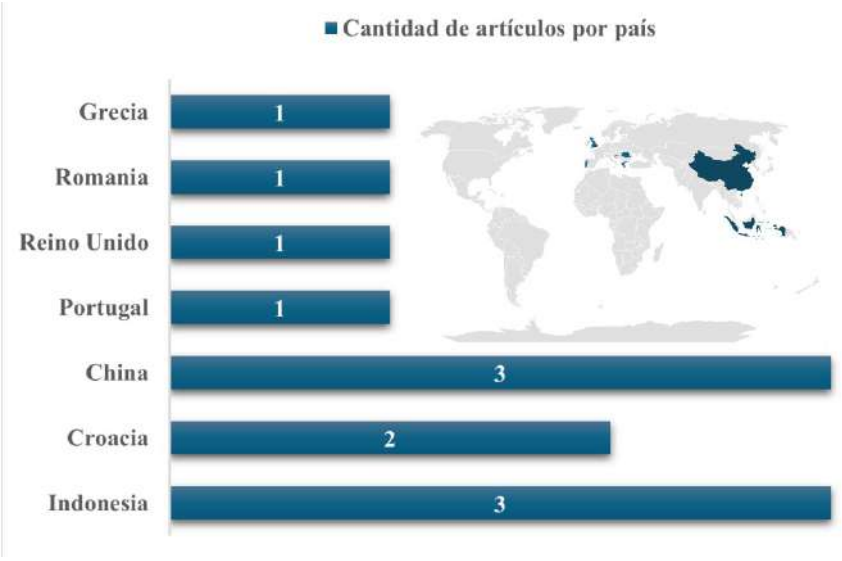
Tabla 1. Artículos seleccionados según los criterios de inclusión y exclusión.

Nro	Autor (res)	Titulo	Año	Principales aportes
1	*Xing Yanbo*	*Design of a Network Security Audit System Based on Log Data Mining*	*2022*	*La investigación analiza el uso de la minería de datos para mejorar la auditoría de seguridad de la red, identificando riesgos ocultos y proporcionando datos auxiliares precisos. (Yanbo, 2022).*
2	*Drogalas G., Karagiorgos D. & Lois P., A., Vrontis, A,Thrassou*	*Internal auditing and cyber security: audit role and procedural contribution*	*2021*	*La seguridad cibernética, es un riesgo creciente, con potenciales pérdidas significativas, donde la auditoría interna es crucial, ya que desempeña un papel activo en proteger los servicios y procesos en línea (Lois et al., 2021).*
3	*Slapničar, S., Vuko, Drašček, M. T., & Čular, M.*	*Effectiveness of cybersecurity audit*	*2022*	*La investigación analiza cómo la efectividad de la auditoría de seguridad cibernética se fortalece con una gestión de riesgos avanzada y se ve desafiada por la probabilidad de ataques cibernéticos exitosos (Slapničar et al., 2022).*
4	*Akma Nurul. & Sudirman*	*Network Penetration a Security Audit Menggunakan Nmap*	*2021*	*La amenaza de ataques externos a los datos es un desafío para las empresas que han digitalizado sus sistemas. Los administradores pueden usar herramientas como Nmap para evaluar y mejorar la seguridad de sus redes mediante la auditoria (Sudirman & Nurul, 2021).*
5	*Saputra, A., Astrida, D. N., & Assaufi, A.*	*Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)*	*2022*	*El estudio identificó, a través de la auditoría, varias vulnerabilidades en la red inalámbrica de una escuela mediante el Estándar de Ejecución de Pruebas de Penetración (PTES). Estos riesgos incluyeron el descifrado de WPA2, ataques de denegación de servicio, descifrado de contraseñas de enrutadores inalámbricos y aislamiento de puntos de acceso (Astrida, Saputra, & Assaufi, 2022).*
6	*Potorac, A, Tudosi, A., Balan, D., & Graur, A.*	*Research on Security Weakness Using Penetration Testing in a Distributed Firewall*	*2023*	*El aumento de la delincuencia cibernética afecta a varias industrias debido a la falta de protección completa. Sin embargo, las auditorías de seguridad periódicas, que incluyen pruebas de penetración y escaneos de vulnerabilidades, pueden ayudar a mitigar este desafío (Tudosi et al., 2023).*

7	Gogolin, F., Rosati, P., & Lynn, T.	Cyber-Security Incidents and Audit Quality	2022	El artículo examina la respuesta de los auditores ante incidentes de seguridad cibernética, destacando un aumento en la realización de pruebas y esfuerzos para enfrentar los riesgos emergentes (Rosati et al., 2022).
8	Ma, H., Wang, L., Li, Z., et al.	A data plane security model of SR-BE/TE based on zero-trust architecture	2022	Se propone un algoritmo de seguridad para auditar redes SR-BE/TE, que se fundamenta en una autenticación sólida. Al analizar bucles, rutas y SID de los mensajes, se pueden detectar amenazas como la manipulación de rutas de transmisión, manipulación de SID y ataques de bucle (Wang, et al., 2022).
9	Maximiano, M., Gomes, R. A. & Antunes, M.	A Client-Centered Information Security and Cybersecurity Auditing Framework	2022	La auditoría busca disminuir la probabilidad de incidentes de seguridad de los datos mediante procedimientos que evalúan medidas de seguridad predefinidas en temas de ciberseguridad y protección de datos (Antunes, Maximiano, & Gomes, 2022).
10	Wenting Wang, Xin Liu, Xiaohong Zhao, Yang Zhao, Rui Wang & Jianpo Li	Design of Intelligent Substation Communication Network Security Audit System	2021	Las subestaciones inteligentes son más vulnerables a ataques debido al aumento de amenazas a la seguridad en las redes de control industrial. Por ello, es crucial fortalecer la evaluación de seguridad de las comunicaciones en para mejorar su protección mediante la auditoria (Wang, et al., 2021).
11	Slapničar, S., Drašček, M., Čular, M. & Vuko, T.,	Key drivers of cybersecurity audit effectiveness: the neo-institutional perspective	2021	Se analizó los elementos que influyen en la eficacia de la auditoría interna en la seguridad de la gestión de riesgos cibernéticos de red. Se sugirió que las regulaciones, la formación académica y las prácticas de externalización contribuyen positivamente a la eficacia de la auditoría de ciberseguridad (Vuko et al., 2021).
12	Rizky, T., & Jenih, J.	Merancang Keamanan Jaringan Internet Menggunakan Program Network Mapper Di Linux Ubuntu	2023	El artículo aborda la constante amenaza de ataques externos y la creciente vulnerabilidad debido al acceso digital, recomendando el uso de herramientas como Nmap para auditorías de seguridad de la red. (Rizky & Jenih, 2023).

En lo que respecta a los países abordados en el estudio de investigación, se evidencia la relevancia de este tema en los continentes asiático y europeo. La Figura 3 muestra la cantidad de investigaciones realizadas por cada país participante en este análisis.

Figura 3. Artículos por país



Efecto de la Auditoría en la Protección de la Red

La auditoría de protección de la red es un elemento fundamental para garantizar la defensa de los sistemas informáticos y alcanzar las metas de seguridad. Como menciona Yanbo (2022), con su implementación de tecnología de minería de datos, la auditoria de seguridad de red no solo permite detectar actividades perjudiciales de manera temprana, sino que también evalúa y analiza vulnerabilidades específicas, identifica posibles ataques y sigue posibles infracciones a las normativas de seguridad, especialmente en este desarrollo continuo de tecnología.

La relevancia de la revisión interna en la protección digital de la red ha sido destacada por diversos autores. Según Lois et al. (2021), subrayan que en un entorno donde la seguridad cibernética representa un riesgo creciente con potenciales pérdidas significativas, la auditoría interna desempeña un papel activo en proteger los servicios y procesos en línea.

Por otro lado, Slapničar et al. (2022), aborda la efectividad de la auditoría de ciberseguridad desde una perspectiva de gestión de riesgos. El desarrollo de un índice de auditoría de ciberseguridad ayuda a las organizaciones a medir y mejorar la madurez de su gestión de riesgos cibernéticos, aunque no necesariamente disminuye la probabilidad de ataques exitosos. Este hallazgo subraya la necesidad de una auditoría continua y adaptativa que pueda responder a las amenazas emergentes.

Las herramientas de auditoría como Nmap son mencionadas por Sudirman y Nurul (2021) y Rizky y Jenih (2023) como recursos importantes para analizar y potenciar la protección de los sistemas de comunicación. Estas herramientas permiten realizar pruebas de penetración y auditorías exhaustivas, identificando posibles vulnerabilidades y fortaleciendo la seguridad de la red.

La auditoría de seguridad de la red desarrolla una función fundamental en la protección de los sistemas informáticos y la prevención de posibles ataques cibernéticos en diversos ámbitos tecnológicos. Mediante la evaluación exhaustiva de vulnerabilidades, la identificación de posibles amenazas y el refuerzo de las medidas de seguridad, la auditoría contribuye significativamente a la seguridad cibernética de una organización.

Discusión

Los hallazgos de este estudio resaltan la importancia crítica de la auditoría de seguridad de la red en la protección de sistemas informáticos y la prevención de ataques cibernéticos. La implementación de auditorías ha demostrado ser una medida efectiva para mejorar la seguridad de la red, identificando y mitigando vulnerabilidades y fortaleciendo la gestión de riesgos cibernéticos.

El uso de herramientas avanzadas como Nmap y la aplicación de técnicas de minería de datos han permitido una detección proactiva de amenazas y una evaluación crítica de las vulnerabilidades existentes. Además, han probado ser valiosas en el análisis y refuerzo de la seguridad de la red, lo que sugiere que su uso podría ser extendido a otras áreas de la ciberseguridad.

Las implicaciones prácticas de estos hallazgos son significativas para la práctica actual de la auditoría de seguridad de la red. La adopción de un enfoque holístico que incluya tanto la evaluación técnica como la colaboración estratégica entre auditores y profesionales de TI podría mejorar la postura de seguridad de las organizaciones. Además, la educación y capacitación constante en ciberseguridad son esenciales para mantenerse al día con las nuevas amenazas y tecnologías.

La auditoría de seguridad de la red es una actividad compleja y multifacética que requiere un enfoque dinámico y proactivo. Los resultados de este estudio subrayan la necesidad de una auditoría continuamente ajustada y adaptable, así como la importancia de la colaboración entre diferentes departamentos dentro de una organización para fortalecer la postura de seguridad de la red.

Conclusiones

Por último, se concluye que la auditoría de seguridad de la red si es un componente fundamental en la protección y preservación de la integridad de los sistemas de computación. Los estudios analizados revelan su papel esencial en la detección temprana de actividades perjudiciales, la evaluación de vulnerabilidades específicas y el seguimiento de posibles infracciones a las normativas de seguridad. Tanto la auditoría interna, al emplear herramientas especializadas como Nmap y las técnicas de minería de datos juegan un papel crucial en el fortalecimiento de la seguridad cibernética y prevención de pérdidas significativas asociadas con los riesgos en constante cambio.

La efectividad de la auditoría no solo depende de las herramientas y técnicas utilizadas, sino también del continuo perfeccionamiento en la gestión de la seguridad informática. La implementación de regulaciones, la formación académica y la externalización se distinguen como factores críticos que contribuyen a su éxito. Sin embargo, en un panorama donde la evolución de las amenazas, la capacidad de adaptación y la respuesta ágil ante incidentes emergen como aspectos esenciales para enfrentar los desafíos actuales en la seguridad de la red.

Es importante reconocer las limitaciones de este estudio. A pesar de que los resultados son prometedores, la investigación se centró en un conjunto específico de artículos, lo que podría limitar la generalización de los hallazgos. Además, la naturaleza en constante evolución de las amenazas cibernéticas significa que los resultados actuales pueden no ser aplicables en el futuro, lo que subraya la necesidad de una investigación continua y adaptativa.

Para futuras investigaciones se podrían explorar nuevas herramientas y técnicas de auditoría que aprovechen las capacidades de la IA y el Machine Learning. Esto permitiría una detección más precisa y una prevención más efectiva de los ataques cibernéticos.

Bibliografía

Antunes, M., Maximiano, M., & Gomes, R.

(2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. Applied Sciences, 12(9), 15. doi: https://dx.doi.org/10.3390/app12094102

ASOBANCARIA. (2022). Guía de buenas prácticas para auditar la ciberseguridad. Recuperado el 02 de marzo de 2024, de https://www.asobancaria.com/wp-content/uploads/2022/06/Guia_de_Buenas_Practicas_para_Auditar_la_Ciberseguridad_2022_V1.pdf

Astrida, D. N., Saputra, A. R., & Assaufi, A. I. (2022). Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES). Sinkron: Jurnal Dan Penelitian Teknik Informatika, 6(1), 147-154. doi: https://doi.org/10.33395/sinkron.v7i1.11249

AWS. (2023). ¿Qué es una red de computadoras? Recuperado el 02 de Marzo de 2023, de https://aws.amazon.com/es/what-is/computer-networking/

Barclay Simpson. (2022). An Introduction to Computer Auditing. Retrieved Marzo 02, 2024, from https://www.barclaysimpson.com/wpcontent/uploads/2022/11/Introduction_to_Computer_Audit2-compressed.pdf

Barquero, W. G. (2022). Análisis de Prisma como Metodología para Revisión Sistemática: una Aproximación General. Saúde em Redes, 8(1), 339–360. doi:https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Canadian Centre for Cyber Security. (n.d.). Network security auditing. Retrieved Marzo 02, 2024, from https://publications.gc.ca/collections/collection_2023/cstc-csec/D97-1-80-086-2022-eng.pdf

Ciapponi, A. (2021). La declaración PRISMA 2020: una guía actualizada para reportar revisiones sistemáticas. Evidencia, actualizacion en la práctica ambulatoria, 24(3), 4. doi: https://dx.doi.org/10.51987/evidencia.v24i4.6960

Koza, K. (2022). Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security Medicon Engineering Themes. Medicon Engineering Themes, 2(3), 14. Retrieved from https://themedicon.com/pdf/engineeringthemes/MCET-02-021.pdf

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. International Journal of Managerial and Financial Accounting, 13(1), 25-47. doi: https://dx.doi.org/10.1504/IJMFA.2021.116207

Morales, F., Simbaña, Y., Coral, R., & Toasa, R. (2021). Technique for Information Security Based on Controls Established by the SysAdmin Audit, Networking and Security Institute. Advances in Intelligent Systems and Computing, 1273, 415-426. doi: https://doi.org/10.1007/978-3-030-59194-6_34

Morán, C., & Maria, J. (2021). Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones. Universidad Politécnica Salesiana. Obtenido de http://dspace.ups.edu.ec/handle/123456789/20568

Najib, M., Purnomosidi, D. B., & Nugroho, M. (2023). IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS MENGGUNAKAN CIS BENCHMARK. Cyber Security dan Forensik Digital, 5(2), 83-88. doi:https://dx.doi.org/10.14421/csecurity.2022.5.2.3929

Rizky, C., & Jenih, J. (2023). Merancang Keamanan Jaringan Internet Menggunakan Program Network Mapper Di Linux Ubuntu. Jurnal Teknologi Informasi, 9(1), 45-55. doi: https://dx.doi.org/10.52643/jti.v9i1.3174

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-Security Incidents and Audit Quality. European Accounting Review, 31(3), 701-728. doi: https://dx.doi.org/10.1080/09638180.2020.1856162

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information

Systems, 44. doi: https://doi.org/10.1016/j.accinf.2021.100548

Sudirman, D., & Nurul, Y. A. (2021). Network Penetration dan Security Audit Menggunakan Nmap. SATIN - Sains Dan Teknologi Informasi, 7(1), 32-44. doi: https://doi.org/10.33372/stn.v7i1.702

Tapia-Benavente, L., Vergara-Merino, L., Ignacio Garegnani, L., Ortiz-Muñoz, L., Loézar Hernández, C., & Vargas-Peirano, M. (2021, 05). Revisiones rápidas: definiciones y usos. Medwave, 21(1), 7. doi: http://dx.doi.org/10.5867/medwave.2021.01.8090

Tsao, K., Girdler, T., & Vassilakis, V. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 39. doi: https://dx.doi.org/10.1016/j.adhoc.2022.102894

Tudosi, A., Graur, A., Balan, D., & Potorac, A. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. Sensors, 23(5), 18. doi: https://doi.org/10.3390/s23052683

Vuko, T., Slapničar, S., Čular, M., & Drašček, M. (2021). Key drivers of cybersecurity audit effectiveness: the neo-institutional perspective. SSRN Electronic Journal. doi: https://doi.org/10.2139/ssrn.3932177

Wang, L., Ma, H., Li, Z., Pei, J., Hu, T., & Zhang, J. (2022). A data plane security model of SR-BE/TE based on zero-trust architecture. Scientific Reports, 12(1), 23. doi: https://dx.doi.org/10.1038/s41598-022-24342-y

Wang, W., Liu, X., Zhao, X., Zhao, Y., Wang, R., & Li, J. (2021). Design of Intelligent Substation Communication Network Security Audit System. Smart Innovation, Systems and Technologies. Singapore. doi: https://doi.org/10.1007/978-981-33-6420-2_48

Wang, Y., Smahi, A., Zhang, H., & Li, H. (2022). Towards Double Defense Network Security Based on Multi-Identifier Network Architecture. Sensors, 22(3), 17. doi: https://doi.org/10.3390/s22030747

Yanbo, X. (2022). Design of a Network Security Audit System Based on Log Data Mining. Wireless Communications and Mobile Computing, 7. doi: https://dx.doi.org/10.1155/2022/6737194