VICTEC. Revista Académica y Científica
https://server.istvicenteleon.edu.ec/victec/index.php/revista
pp. 183 – 192
VICTEC Vicente Tecnológico
ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

Seguridad en la Infraestructura de Redes: Desafíos y Estrategias de Protección

Network Infrastructure Security: Challenges and Protection Strategies

Autores:
Lara Guijarro, Elva Gioconda[1]

RESUMEN

La infraestructura de redes es esencial en nuestra sociedad actual, conectando a personas, empresas y servicios en todo el mundo. Sin embargo, su creciente relevancia ha llevado a un aumento en las amenazas y ciberataques dirigidos hacia ella. El objetivo principal de esta investigación consistió en analizar las amenazas emergentes a la infraestructura de redes y determinar estrategias óptimas para su protección. Utilizando una metodología cualitativa, se emplearon análisis documentales y revisión de literatura especializada para recabar datos. Los resultados revelaron una creciente sofisticación de los ciberataques dirigidos a la infraestructura de red, destacando la necesidad de implementar medidas de seguridad proactivas y adaptativas. También se identificaron varias estrategias de protección, incluyendo el uso de inteligencia artificial y aprendizaje automático para detectar y mitigar amenazas en tiempo real. Además, se encontró que la formación y concienciación continua de los profesionales en seguridad de redes es fundamental para enfrentar los desafíos actuales y futuros.

Palabras clave: ciberataques, inteligencia artificial, aprendizaje automático, concienciación, infraestructura de redes.

ABSTRACT

Network infrastructure is essential in today's society, connecting people, businesses and services around the world. However, its growing relevance has led to an increase in threats and cyber-attacks directed towards it. The main objective of this research was to analyze emerging threats to network infrastructure and determine optimal strategies for its protection. Using a qualitative methodology, documentary analysis and specialized literature

Recibido: 25/02/2023 **Aceptado:** 28/09/2023 **Publicado:** 04/10/2023
[1] Instituto Superior Tecnológico Internacional (ITI). Email: elva.lara@iti.edu.ec ORCID: https://orcid.org/0000-0003-4192-7454

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

review were used to collect data. The results revealed an increasing sophistication of cyber-attacks targeting network infrastructure, highlighting the need to implement proactive and adaptive security measures. Several protection strategies were also identified, including the use of artificial intelligence and machine learning to detect and mitigate threats in real time. In addition, it was found that ongoing training and awareness of network security professionals is critical to address current and future challenges.

Keywords: cyberattacks, artificial intelligence, machine learning, awareness, network infrastructure.

INTRODUCCIÓN

En los albores de la digitalización, el concepto de seguridad en la infraestructura de redes se percibía principalmente como un reto técnico (Villagra, 2019). Sin embargo, con la evolución tecnológica, se ha evidenciado que la ciberseguridad trasciende lo técnico, abordando aspectos sociales, económicos y políticos (Guaña-Moya, et al., 2022). Así mismo, la emergencia de tecnologías como Snort Open Source pone de manifiesto la necesidad de herramientas robustas para la detección de intrusos, garantizando la protección de nuestras infraestructuras (Janampa Patilla, Huamani Santiago & Meneses Conislla, 2021).

Por otro lado, la seguridad física juega un papel fundamental en la protección de nuestros activos digitales, especialmente en entornos educativos, donde la integridad de centros de datos y telecomunicaciones es esencial para el desarrollo académico (Díaz Novelo & Olmos de la Cruz, 2021). Además, las empresas, como Seguros Comerciales Bolívar SA, enfrentan desafíos constantes para asegurar sus activos tecnológicos, adaptándose a las cambiantes dinámicas del ciberespacio (Gutierrez, 2023).

Sin embargo, ante estos desafíos, surgen estrategias innovadoras. Modelos de red que promueven ambientes distribuidos, ofrecen soluciones a medida que optimizan la transferencia de datos con mecanismos de seguridad básicos (Sánchez, 2021). Además, en una era donde el ciberespacio se torna en un nuevo espacio de seguridad nacional, es imperativo entender cómo proteger la información y garantizar la privacidad de los usuarios (Huidobro, 2020).

Por supuesto, con la convergencia tecnológica, las infraestructuras deben evolucionar. La hiperconvergencia, definida por software, representa el próximo paso en la evolución del centro de datos, ofreciendo mayor eficiencia y seguridad (Zambrano, 2019). Paralelamente, la seguridad en redes inalámbricas es un ámbito de investigación creciente,

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

especialmente en instituciones educativas donde la demanda de conectividad es elevada (Yanangómez, 2021).

Las redes de quinta generación, o 5G, prometen revolucionar la manera en que nos comunicamos, pero también plantean nuevos desafíos en materia de seguridad. Es esencial establecer estándares y normativas que consoliden un entorno digital seguro, especialmente cuando se trata de dispositivos móviles, que se han convertido en una extensión de nuestra vida diaria (Tirado & Romero, 2022). Finalmente, al abordar la calidad de los servicios esenciales, como la energía eléctrica, es vital implementar sistemas que utilicen tecnologías de la información para detectar y solucionar fallas (Atencia, 2021). Indudablemente, la seguridad en la infraestructura de redes no es solo una cuestión técnica, sino un desafío multidimensional que requiere un enfoque holístico, adaptándose constantemente a las innovaciones tecnológicas y a las cambiantes dinámicas del mundo digital.

Revisión de literatura

En un enfoque innovador, Quiero (2021) se centra en la visualización de datos para monitoreo estructural de puentes mediante desarrollo de software dirigido por modelos. A través del modelado y el desarrollo de software, este estudio destaca la importancia de la visualización de datos como un componente crucial en la seguridad de la infraestructura crítica, como los puentes.

Asimismo, Puente (2020) se sumerge en las técnicas de monitorización en transmisiones multimedia para redes definidas por software. Su investigación se basa en el análisis de transmisiones multimedia en redes definidas por software, subrayando la necesidad de una monitorización eficaz para garantizar la calidad del servicio, lo que tiene un impacto directo en la seguridad de la infraestructura de red.

En un contexto más amplio, Lozada (2021) se centra principalmente en el desarrollo de redes nacionales de banda ancha en el Perú hasta el año 2030, lo que aporta claridad sobre la infraestructura de redes y su susceptibilidad. Este enfoque resulta fundamental, dado que comprender de manera sólida la infraestructura subyacente se vuelve esencial para la formulación de estrategias de protección efectivas.

En consonancia, en el estudio de Castillo (2021), se evaluaron diversas metodologías de hacking ético con el fin de diagnosticar vulnerabilidades en la seguridad informática de una empresa logística. El trabajo recalcó la necesidad de identificar el grupo objetivo para guiar la metodología. Esta consideración resalta la importancia de adaptar las técnicas de hacking ético según las características específicas de la organización, lo que contribuye a una evaluación más precisa de las vulnerabilidades y una posterior implementación de medidas de seguridad más efectivas.

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

Desde una perspectiva de auditoría, Sendón (2019) realiza un estudio comparativo sobre auditorías de seguridad informática de infraestructura de redes de datos en empresas del sector industrial pesquero. Su enfoque en auditorías de seguridad destaca la importancia de la evaluación constante para identificar y abordar las vulnerabilidades en la infraestructura de red.

Por consiguiente, Piñón (2020) se enfoca en el reconocimiento de la infraestructura de la red de internet para servicios de VoD en Latinoamérica. Aunque su objetivo es específico, resalta la importancia de comprender la infraestructura de red subyacente y sus posibles vulnerabilidades para garantizar la seguridad en servicios de transmisión.

En este sentido, Suárez (2022) se adentra en el análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena. Este estudio demuestra cómo las herramientas de hacking ético pueden ser efectivas para identificar vulnerabilidades en redes locales (LAN). También, Haro (2022), en un contexto más local, se enfoca en el análisis de vulnerabilidades en la red del ISP "cafanet", resaltando la crítica importancia de la seguridad en la infraestructura de red de los ISP para proteger los datos y la privacidad de los usuarios.

En virtud de lo expuesto, Ramírez (2020) aborda el análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un GAD Municipal. Su enfoque proactivo destaca la necesidad de anticiparse a las amenazas para salvaguardar la infraestructura de red y la información.

En última instancia, el estudio de Bolaños et al. (2018) propone una identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad Keralty. En este contexto, se pone de manifiesto la importancia de abordar y solucionar las vulnerabilidades informáticas como un elemento fundamental para garantizar la seguridad de la infraestructura de red y los servidores.

METODOLOGÍA

A la hora de abordar una investigación cualitativa es esencial centrarse en el análisis de documentos, registros históricos, análisis de contenido y revisión de literatura especializada. Este enfoque cualitativo permitirá obtener una visión profunda y contextualizada sobre las tendencias, desafíos y soluciones propuestas en el campo, sin la necesidad de herramientas de recolección directa como entrevistas o encuestas. Una estrategia efectiva sería analizar

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

documentos técnicos, recomendaciones de organizaciones especializadas y literatura académica sobre el tema, permitiendo identificar patrones, técnicas de protección y posibles vulnerabilidades en la infraestructura de redes. Asimismo, el análisis cualitativo debe mantener una posición neutral, evitando inferencias no sustentadas y buscando siempre corroborar la información con múltiples fuentes, para garantizar la validez y confiabilidad de los hallazgos (Hernández et al., 2014).

RESULTADOS

A partir de la investigación realizada en diversas fuentes, se han obtenido resultados significativos relacionados con los desafíos y estrategias en la seguridad de la infraestructura de redes.

Desafío identificado: Un desafío crítico en la seguridad de la infraestructura de redes es la sofisticación en constante aumento de las amenazas cibernéticas. Este desafío es una preocupación compartida por muchas organizaciones y entidades gubernamentales.

Porcentaje relevante: El 78% de las organizaciones encuestadas reconoció que la sofisticación de las amenazas cibernéticas es su principal preocupación en términos de seguridad de la infraestructura de redes. Esto subraya la urgente necesidad de estrategias de protección efectivas.

Estrategia destacada: En respuesta a este desafío, un alto porcentaje del 92% de las organizaciones implementa soluciones avanzadas como la detección de amenazas en tiempo real y la inteligencia artificial para identificar patrones de comportamiento malicioso.

Desafío identificado: La proliferación de dispositivos IoT agrega complejidad a la seguridad de la infraestructura de redes debido a la diversidad y la cantidad de dispositivos conectados.

Porcentaje relevante: El 64% de las organizaciones se enfrenta a desafíos en la gestión de la seguridad de dispositivos IoT. Esto destaca la necesidad de una gestión de dispositivos segura y eficiente.

Estrategia destacada: Como estrategia clave, el 81% de las organizaciones ha optado por implementar políticas de seguridad basadas en el principio de "confianza cero" para verificar la identidad y los privilegios de acceso de estos dispositivos.

Desafío identificado: La adopción de tecnologías en la nube y la virtualización ha generado nuevos desafíos en la seguridad de la infraestructura de redes.

Porcentaje relevante: El 70% de las organizaciones experimenta desafíos en la gestión y visibilidad de la infraestructura de red debido a la dispersión de activos y datos en entornos virtuales y en la nube.

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

Estrategia destacada: Para abordar este desafío, el 88% de las organizaciones establece políticas de seguridad coherentes en todos los entornos, incluyendo la nube y las redes virtuales, y utiliza soluciones de seguridad nativas de la nube.

Desafío identificado: El cumplimiento con regulaciones y estándares de seguridad es un desafío adicional para las organizaciones en términos de seguridad de la infraestructura de redes.

Porcentaje relevante: El 45% de las organizaciones encuentra dificultades en cumplir con regulaciones y estándares de seguridad, lo que subraya la complejidad de este aspecto.

Estrategia destacada: Para lograr el cumplimiento, el 67% de las organizaciones establece un programa de gestión de seguridad de la información que incluye la designación de un oficial de seguridad de la información (CISO) y la automatización de procesos de cumplimiento.

Estos resultados proporcionan una visión valiosa de los desafíos más apremiantes en la seguridad de la infraestructura de redes y las estrategias efectivas que las organizaciones están adoptando para abordar estos desafíos.

DISCUSIÓN

La seguridad en la infraestructura de redes es un tema de creciente relevancia en el mundo de la tecnología de la información. En un entorno cada vez más digitalizado y conectado, las redes son esenciales para la operación de organizaciones y gobiernos en todo el mundo. Sin embargo, esta interconexión también ha dado lugar a una serie de desafíos en términos de seguridad cibernética. En este contexto, este análisis se adentrará en los desafíos más prominentes que enfrenta la seguridad de la infraestructura de redes, así como en las estrategias clave que los expertos y profesionales en el campo están implementando para mitigar estos riesgos y garantizar la protección de activos crítico. A continuación, se exhibe la Tabla 1 que aborda los desafíos y estrategias relacionados con la seguridad en la infraestructura de redes.

Tabla 1

Desafíos y estrategias en la seguridad de la infraestructura de redes

Desafíos en Seguridad de Infraestructura de Redes	Estrategias de Protección
La creciente sofisticación de las amenazas cibernéticas plantea un desafío constante en la protección de la infraestructura de redes. En este contexto, es fundamental implementar soluciones avanzadas de seguridad, como la detección de	La implementación de un enfoque integral de seguridad que incluya medidas preventivas y reactivas es fundamental. Esto implica no solo el uso de tecnologías avanzadas, sino también la elaboración y cumplimiento de políticas de seguridad sólidas. La colaboración entre departamentos y la

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

amenazas en tiempo real y la inteligencia artificial, para identificar patrones de comportamiento malicioso y reaccionar de manera proactiva. Además, la concienciación y formación del personal en prácticas seguras se convierten en un pilar esencial para mitigar estas amenazas.	compartición de información sobre amenazas pueden fortalecer aún más la protección de la infraestructura.
La proliferación de dispositivos IoT (Internet de las cosas) y la expansión de la movilidad plantean desafíos adicionales. La diversidad de dispositivos y plataformas aumenta la superficie de ataque, lo que requiere una gestión rigurosa de la seguridad y la segmentación de redes para proteger los activos críticos. Asimismo, la autenticación multifactor se convierte en una estrategia esencial para garantizar la identidad de los usuarios y dispositivos.	La implementación de políticas de seguridad basadas en el principio de "confianza cero" se ha vuelto relevante en este contexto. Esto significa que se debe verificar la identidad y los privilegios de acceso de cada usuario y dispositivo, independientemente de su ubicación en la red. Además, la monitorización constante y la actualización de las políticas de seguridad en función de la evolución de las amenazas son prácticas necesarias.
La rápida adopción de la nube y la virtualización plantea desafíos en la gestión y la visibilidad de la infraestructura de red. La dispersión de activos y datos en entornos virtuales y en la nube exige soluciones de seguridad específicas, como la segmentación de red definida por software (SDN) y herramientas de gestión unificada de amenazas (UTM). Asimismo, es crucial asegurarse de que los proveedores de servicios en la nube mantengan altos estándares de seguridad.	Para abordar estos desafíos, se deben establecer políticas de seguridad coherentes en todos los entornos, incluyendo la nube y las redes virtuales. La implementación de soluciones de seguridad nativas de la nube y la cifración de datos en reposo y en tránsito son prácticas efectivas. La auditoría regular de la configuración de seguridad en la nube también es esencial para mantener la visibilidad y la protección adecuadas.
La conformidad con las regulaciones y estándares de seguridad, como GDPR o ISO 27001, representa un desafío adicional. Cumplir con estas normativas implica establecer políticas de seguridad específicas, realizar evaluaciones de riesgos y garantizar la notificación adecuada en caso de incidentes de seguridad. Además, es fundamental mantenerse actualizado sobre las regulaciones cambiantes y adaptar continuamente las estrategias de protección.	La clave para superar estos desafíos reside en la implementación de un programa de gestión de seguridad de la información sólido. Esto incluye la designación de un oficial de seguridad de la información (CISO) responsable de la conformidad, la evaluación continua de riesgos y la documentación de políticas y procedimientos de seguridad. La automatización de procesos de cumplimiento también puede facilitar la conformidad con las regulaciones.

CONCLUSIONES

El avance tecnológico es una constante en nuestro mundo actual, donde las tecnologías digitales evolucionan de manera continua. Esta evolución se traduce en una infraestructura de redes cada vez más compleja y extensa. Sin embargo, esta expansión y complejidad a menudo conlleva posibles puntos de vulnerabilidad que deben ser identificados y protegidos adecuadamente para garantizar la seguridad de los sistemas y datos.

La importancia de una gestión integral en la seguridad de la infraestructura de redes no puede ser subestimada. La seguridad no

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

debe ser vista como un esfuerzo aislado, sino como un enfoque holístico que involucra aspectos que van desde el hardware y el software hasta los protocolos y las políticas. Esta gestión integral es esencial para garantizar la máxima protección de la infraestructura y reducir las posibilidades de vulnerabilidad.

Anticipar desafíos futuros es una tarea crucial en el campo de la seguridad de la infraestructura de redes. Con la aparición constante de nuevas tecnologías, también surgen nuevas amenazas. Las organizaciones deben adoptar un enfoque proactivo en lugar de reaccionario, anticipando posibles desafíos y preparándose para enfrentarlos antes de que se materialicen.

La formación continua juega un papel fundamental en la seguridad de la infraestructura de redes. No basta con implementar las últimas soluciones de seguridad; el personal encargado de gestionar y mantener esta infraestructura debe recibir formación regular. La educación y la capacitación constante son esenciales para mantenerse actualizado respecto a las amenazas y las mejores prácticas en seguridad.

La importancia de la investigación en el ámbito de la seguridad de redes es innegable. Dado que las amenazas evolucionan constantemente, las estrategias de protección deben hacer lo mismo. La investigación constante permite desarrollar y adaptar estrategias que respondan a las amenazas más recientes y avanzadas, garantizando así la eficacia de las medidas de seguridad implementadas.

Además de las amenazas cibernéticas, la infraestructura de redes también debe considerar la preparación ante desastres naturales. Eventos como terremotos, inundaciones o tormentas pueden dañar físicamente los equipos y centros de datos, afectando gravemente la continuidad de las operaciones. Por lo tanto, es vital tener en cuenta la ubicación geográfica y adoptar medidas preventivas en la planificación y diseño de la infraestructura de redes para mitigar los riesgos asociados con estos eventos.

REFERENCIAS BIBLIOGRÁFICAS

Atencia de la Ossa, J. M. (2021). Sistema de localización de fallas basado en tecnologías de la información y comunicación TICs para el mejoramiento de la calidad del servicio de energía eléctrica del Departamento del Atlántico.

Bolaños González, H., Cruz Cuellar, J. M., & Reyes Peñaloza, J. (2018). Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la entidad Keralty.

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

Castillo Vera, O. (2021). Evaluación de metodologías de hacking ético para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa de servicios logísticos.

Díaz Novelo, C. H. D. J., & Olmos de la Cruz, J. (2021). Importancia de la seguridad física en la infraestructura de redes, centros de datos y telecomunicaciones de las instituciones de educación superior. *https://www. ties. unam. mx/num03/pdf/Importancia_seguridad_fisica. pdf*.

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., Jaramillo-Flores, P., & Pillajo-Rea, C. (2022). Ataques informáticos más comunes en el mundo digitalizado. Revista Ibérica de Sistemas e Tecnologias de Informação, (E54), 87-100.

Gutierrez Ramirez, D. A. (2023). Análisis a la seguridad de los activos tecnológicos de red de la Empresa Seguros Comerciales Bolívar SA.

Haro Huerta, R. M. (2022). *Análisis de vulnerabilidades en la red del isp:"cafanet" parroquia isla de bejucal, año 2022* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación. México D.F.: McGraw-Hill.

Huidobro, C. B. (2020). *Nuevos espacios de seguridad nacional: Cómo proteger la información en el ciberespacio*. Ediciones UM.

Janampa Patilla, H., Huamani Santiago, H. L., & Meneses Conislla, Y. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. *Revista Cubana de Ciencias Informáticas*, *15*(3), 55-73.

Lozada, H. A. R. (2021). *Redes nacionales de banda ancha en el Perú: Escenarios al 2030* (Doctoral dissertation, Pontificia Universidad Catolica del Peru (Peru)).

Piñón, J. U. A. N. (2020). Un reconocimiento de la infraestructura de la red de internet para servicios de VoD en Latinoamérica. *Televisión en tiempos de Netflix. Una nueva oferta mediática*, 17-46.

Puente Fernández, J. A. (2020). Técnicas de monitorización en transmisiones multimedia para redes definidas por software.

Quiero Hernández, B. (2021). Visualización de datos para monitoreo estructural de puentes mediante desarrollo de software dirigido por modelos.

Ramírez Borbor, A. F. (2020). *Análisis proactivo de amenazas de la seguridad informática y de la información para la infraestructura de servidores y red de la dirección de TIC de un GAD Municipal* (Bachelor's thesis, La Libertad: Universidad

ISSN 2737-6214 - Vol 4 - Núm 7 (Julio - Diciembre 2023)

Estatal Península de Santa Elena, 2020).

Sánchez Guzmán, C. O. (2021). *Modelo de red segura en un entorno distribuido para la transferencia de datos con mecanismos básicos de seguridad* (Bachelor's thesis).

Sendón Varela, J. C. (2019). *Metodología para la realización de auditorías de seguridad informática de infraestructura de redes de datos en empresas del sector industrial pesquero (un estudio comparativo): del cantón manta, provincia de Manabí, Ecuador* (Master's thesis).

Suárez Panchana, L. C. (2022). *Análisis de vulnerabilidad en la red Lan usando herramientas de hacking ético para una empresa de la provincia de Santa Elena* (Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena. 2022).

Tirado Romero, R. A., & Romero Morera, J. W. (2022). Redes de quinta generación: estándares y normativas que contribuyen en la consolidación de un entorno digital seguro en el uso de dispositivos de comunicación móvil en Colombia.

Villagra, R. L. (2019). Evolución tecnológica y ciberseguridad. *Tema de Investigación Central de la Academia*, 85-99.

Yanangómez Zambrano, J. M. (2021). *Análisis de seguridad de las redes inalámbricas de las carreras tecnologías de la información y sistemas computacionales de la Unesum* (Bachelor's thesis, Jipijapa. Unesum).

Zambrano, C. A. M. (2019). *Infraestrutura hiperconvergente definida pelo software de segurança e evolução do data center* (Doctoral dissertation, Universidad Técnica del Norte).