Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Seguridad y privacidad en las redes 5g: una revisión sistemática de la literatura
Security and privacy in 5g networks: a systematic literature review

Yajaira Noemí Bravo Delgado, David Fernando Zambrano Montenegro

CIENCIA E INNOVACIÓN EN DIVERSAS DISCIPLINAS CIENTÍFICAS.
Julio - Diciembre, V°5-N°2; 2024

✓ **Recibido:** 10/07/2024
✓ **Aceptado**: 16/07/2024
✓ **Publicado:** 31/12/2024

PAIS

- Portoviejo, Ecuador
- Portoviejo, Ecuador

INSTITUCIÓN:

- Universidad Técnica de Manabí
- Universidad Técnica de Manabí

CORREO:

ybravo4835@utm.edu.ec
david.zambrano@utm.edu.ec

ORCID:

https://orcid.org/0009-0002-8108-9061
https://orcid.org/0000-0002-8833-1546

FORMATO DE CITA APA.

Bravo, Y. Zambrano, D. *(2024). Seguridad y privacidad en las redes 5g: una revisión sistemática de la literatura. Revista G-ner@ndo, V°5 (N°2,). 116 -144.*

Resumen

Este artículo presenta una investigación documental que aborda los desafíos de seguridad y privacidad en las redes 5G mediante una revisión sistemática de la literatura. Utilizando la metodología PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), se llevó a cabo un análisis detallado de estudios publicados desde 2019 en bases de datos científicas como IEEE Xplore, ACM Digital Library y SpringerLink. Se identificaron 28 amenazas principales, incluyendo violaciones de datos, ataques de IoT y amenazas internas, así como estrategias como el análisis de seguridad impulsado por IA y el uso de blockchain para mitigar estos riesgos. Las tendencias emergentes incluyen la integración de inteligencia artificial para la detección de amenazas y la mejora continua del cifrado de datos. Este estudio subraya la necesidad de desarrollar estándares robustos y mecanismos de consentimiento del usuario efectivos para proteger la privacidad en las redes 5G. Se identificaron áreas para futuras investigaciones, como la criptografía cuántica y la validación empírica de soluciones propuestas en diversos contextos de implementación.

Palabras clave: Redes 5G, seguridad, privacidad, revisión sistemática, tendencias emergentes.

Abstract

This article presents desk research that addresses security and privacy challenges in 5G networks through a systematic literature review. Using the PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) methodology, a detailed analysis of studies published since 2019 in scientific databases such as IEEE Xplore, ACM Digital Library and SpringerLink was carried out. 28 top threats were identified, including data breaches, IoT attacks, and insider threats, as well as strategies such as AI-powered security analysis and the use of blockchain to mitigate these risks. Emerging trends include the integration of artificial intelligence for threat detection and continuous improvement of data encryption. This study highlights the need to develop robust standards and effective user consent mechanisms to protect privacy in 5G networks. Areas for future research were identified, such as quantum cryptography and empirical validation of proposed solutions in various implementation contexts.
Keywords: 5G networks, security, privacy, systematic review, emerging trends.

Keywords: Mobile applications, data privacy and privacy preservation techniques.

Introducción

En la era actual de rápidos avances tecnológicos, la implementación de las redes 5G ha sido un punto de inflexión significativo en el ámbito de las comunicaciones. Según Gallego Vara (2021), la promesa de una conectividad ultrarrápida y masiva ha generado una transformación sustancial en la forma en que nos comunicamos y accedemos a la información. Sin embargo, este progreso tecnológico no está exento de desafíos críticos, y es en este contexto que se enfoca la presente investigación. El propósito central de este estudio es realizar una revisión sistemática de la literatura para abordar los desafíos asociados con la seguridad y privacidad en la implementación de las redes 5G. A través de una exploración integral de los estudios existentes, se busca identificar las amenazas cibernéticas más destacadas, analizar los enfoques y estrategias de seguridad propuestos, y detectar posibles brechas en el conocimiento que puedan guiar futuras investigaciones.

La importancia de abordar la seguridad y privacidad en las redes 5G radica en su papel esencial en la sociedad digital actual. Desde la comunicación diaria hasta la gestión de dispositivos inteligentes, estas redes se han convertido en el eje central de la conectividad. En este contexto, garantizar la seguridad y privacidad de la información se vuelve imperativo, y esta investigación busca contribuir a ese entendimiento. Con la adopción masiva de las redes 5G, la sociedad se enfrenta a nuevos desafíos y riesgos que deben ser comprendidos y gestionados de manera efectiva. Este estudio se sitúa en la vanguardia de la investigación, abordando los desafíos contemporáneos en seguridad y privacidad, proporcionando así una base sólida para la toma de decisiones informadas en este entorno tecnológico dinámico. Este trabajo busca aportar a la comprensión integral de los desafíos de seguridad y privacidad en las redes 5G, ofreciendo conocimientos valiosos para la toma de decisiones informadas y el desarrollo de estrategias efectivas en este contexto tecnológico en constante evolución.

González (2020) menciona que, en la última década, la evolución de las tecnologías de comunicación ha sido testigo de la implementación progresiva de redes 5G, marcando un hito significativo en la conectividad global. Este avance ha promovido una revolución en la forma en que interactuamos con la información y los dispositivos conectados, pero a su vez ha suscitado preocupaciones críticas en torno a la seguridad y privacidad de estos entornos de comunicación avanzados. Además, Neninger y Guerrero (2023) argumentan que se destaca la necesidad de abordar los desafíos de seguridad inherentes a las redes 5G, considerando la multiplicidad de dispositivos conectados y la transferencia masiva de datos. La implementación global de redes 5G ha generado interrogantes sobre cómo las amenazas cibernéticas y las vulnerabilidades podrían amplificarse en este nuevo contexto tecnológico. En un nivel más específico, algunos autores advierten sobre la necesidad de comprender y abordar los riesgos de privacidad asociados con la vasta cantidad de datos generados por las redes 5G asi lo indica Lecuit (2020). Este planteamiento amplio destaca la importancia de explorar a fondo la literatura disponible para identificar las amenazas específicas, estrategias de seguridad y brechas en el conocimiento que rodean la implementación de redes 5G.

El problema que motiva esta investigación se centra en la falta de una revisión sistemática que aborde integralmente los desafíos de seguridad y privacidad en las redes 5G. A medida que estas redes se despliegan a escala mundial, es esencial comprender y mitigar los riesgos asociados. La hipótesis a defender sugiere que la revisión sistemática revelará patrones críticos en las amenazas cibernéticas, estrategias de seguridad y áreas insuficientemente investigadas, proporcionando una base sólida para futuras investigaciones y prácticas de implementación segura. En términos geográficos, esta investigación no se limitará a una ubicación específica, ya que los desafíos de seguridad y privacidad en las redes 5G trascienden fronteras geográficas. La relevancia de esta investigación se destaca al reconocer que la seguridad y privacidad en las redes 5G son preocupaciones que deben ser abordadas de manera integral y global.

Este trabajo se propone llevar a cabo una revisión sistemática de la literatura centrada en los desafíos de seguridad y privacidad asociados con estas redes de próxima generación. La investigación se enfocará en recopilar, analizar y sintetizar la literatura existente para identificar las amenazas cibernéticas más destacadas y evaluar los enfoques de seguridad y privacidad propuestos en el contexto de las redes 5G. La realización de esta revisión sistemática tiene como objetivo proporcionar una comprensión profunda de los riesgos y desafíos específicos en materia de seguridad y privacidad que surgen con la implementación de las redes 5G. Esta información es esencial para informar las decisiones estratégicas en el desarrollo y despliegue de estas redes, así como para orientar futuras investigaciones en este campo crítico.

La metodología de la revisión sistemática permitirá una exploración exhaustiva de la literatura científica y técnica pertinente. Se llevará a cabo un análisis riguroso de los estudios existentes, identificando patrones, tendencias y brechas en el conocimiento para proporcionar una visión completa de los desafíos de seguridad y privacidad en las redes 5G. Los beneficiarios directos de este trabajo incluyen los profesionales en el ámbito de las telecomunicaciones, investigadores, responsables de políticas tecnológicas y empresas involucradas en el desarrollo y despliegue de redes 5G. Además, la sociedad en general se beneficia al obtener una comprensión más clara de los desafíos de seguridad y privacidad en la era de las redes 5G, permitiendo una adopción más informada y segura de estas tecnologías.

Jiménez (2020) señala que la seguridad de las redes 5G se sustenta en tres pilares fundamentales: la salvaguarda de la privacidad de los usuarios, la seguridad de la virtualización y la protección de los miles de nuevos dispositivos interconectados. Se focaliza en combatir uno de los ataques más destacados dirigidos a las tecnologías móviles: el IMSI Catcher. Este tipo de ataque persigue la sustracción de la identidad del abonado, o IMSI, con el objetivo de determinar su ubicación y facilitar la ejecución de diversos ataques a partir de la obtención de este número. El análisis de elementos fundamentales en la seguridad de redes inalámbricas abarca aspectos

como protocolos de seguridad, vulnerabilidades y ataques recurrentes. Se investigan las debilidades comunes presentes en protocolos de encriptación, como WEP y WPA, que han sido blanco de ataques de fuerza bruta y explotación de vulnerabilidades. Simultáneamente, se identifican protocolos más robustos, como el WPA2 y WPA3, los cuales han experimentado mejoras significativas, fortaleciendo considerablemente la resistencia frente a posibles ataques según lo afirman Basurto y Guaña (2023). Se destaca de manera efectiva la vulnerabilidad de protocolos como WEP y WPA, al tiempo que se reconoce la mejora sustancial en la resistencia proporcionada por protocolos más seguros como WPA2 y WPA3. Los estándares técnicos de las recientes redes 5G, impulsados por la rápida innovación tecnológica en busca de liderar el mercado, no han abordado de manera suficiente cuestiones cruciales como la ciberseguridad, la interoperabilidad, la certificación, la identidad, así como la salvaguarda de la privacidad y la confidencialidad de las comunicaciones móviles (Lecuit, 2020). El 5G se ha posicionado, junto con la inteligencia artificial, como uno de los habilitadores digitales más importantes que facilitarán la disrupción digital. Mora, Rodríguez y Caro (2022) encontraron que analizar los desafíos y proponer enfoques de solución en el ámbito de la ciberseguridad en las redes 5G implica la identificación de amenazas avanzadas que enfrentan estas redes, la consideración de la vulnerabilidad de dispositivos IoT, la protección de la privacidad de datos y la respuesta a la escasez de expertos en ciberseguridad. Por otro lado, Celín (2019) indica que la importancia de las tecnologías Blockchain y 5G en los ámbitos académico y científico destaca sus amplias aplicaciones, sugiriendo su potencial para transformar la interacción y las transacciones tanto en el ámbito personal como en el sector privado.

Sharma y Chen (2019) sostienen que la evolución de las redes de telecomunicaciones ha sido crucial para el desarrollo de la sociedad digital. Desde la primera generación (1G) hasta la cuarta generación (4G), cada salto tecnológico ha traído mejoras significativas en la capacidad y velocidad de transmisión de datos, así como en la cobertura y calidad de los servicios móviles.

Sin embargo, la quinta generación (5G) se presenta no solo como una mejora incremental, sino como una revolución en el ámbito de las telecomunicaciones, proporcionando una infraestructura que soporta una gran variedad de aplicaciones y servicios avanzados, incluyendo el Internet de las Cosas (IoT), la realidad aumentada y virtual (AR/VR), y los vehículos autónomos. El despliegue de las redes 5G implica una serie de innovaciones tecnológicas como la utilización de bandas de frecuencia más altas (milimétricas), la implementación de redes definidas por software (SDN), la virtualización de funciones de red (NFV) y la introducción de la arquitectura de red de acceso múltiple (MEC) (González, 2020). Estas características permiten una mayor flexibilidad y eficiencia en la gestión de los recursos de red, así como una mejora significativa en la latencia y el ancho de banda disponibles para los usuarios, como lo explican Choi, Kim y Lee (2019).

Taleb et al. (2019) describen que, a pesar de los numerosos beneficios, la introducción de 5G también plantea importantes desafíos en términos de seguridad y privacidad. Las características avanzadas de 5G, como la virtualización y la mayor cantidad de puntos de entrada para dispositivos IoT, amplían la superficie de ataque y pueden incrementar la vulnerabilidad de la red frente a diversas amenazas. Por otra parte, Potlapally y Veeramachaneni (2020) comentan que la seguridad en 5G debe abordar múltiples capas, desde la infraestructura física hasta las aplicaciones y servicios que operan sobre la red. La autenticación robusta, el cifrado de datos, la integridad y disponibilidad del servicio, y la gestión segura de identidades son aspectos críticos que requieren atención especial. La seguridad de las redes 5G se sustenta en tres pilares fundamentales: la salvaguarda de la privacidad de los usuarios, la seguridad de la virtualización y la protección de los miles de nuevos dispositivos interconectados. Se focaliza en combatir uno de los ataques más destacados dirigidos a las tecnologías móviles: el IMSI Catcher. Este tipo de ataque persigue la sustracción de la identidad del abonado, o IMSI, con el objetivo de determinar

su ubicación y facilitar la ejecución de diversos ataques a partir de la obtención de este número (Kaloxylos, 2019).

Jiménez (2020) menciona que el análisis de elementos fundamentales en la seguridad de redes inalámbricas abarca aspectos como protocolos de seguridad, vulnerabilidades y ataques recurrentes. Se investigan las debilidades comunes presentes en protocolos de encriptación, como WEP y WPA, que han sido blanco de ataques de fuerza bruta y explotación de vulnerabilidades. Simultáneamente, se identifican protocolos más robustos, como el WPA2 y WPA3, los cuales han experimentado mejoras significativas, fortaleciendo considerablemente la resistencia frente a posibles ataques. Se destaca de manera efectiva la vulnerabilidad de protocolos como WEP y WPA, al tiempo que se reconoce la mejora sustancial en la resistencia proporcionada por protocolos más seguros como WPA2 y WPA3. Basurto y Guaña (2023) afirman que los estándares técnicos de las recientes redes 5G, impulsados por la rápida innovación tecnológica en busca de liderar el mercado, no han abordado de manera suficiente cuestiones cruciales como la ciberseguridad, la interoperabilidad, la certificación, la identidad, así como la salvaguarda de la privacidad y la confidencialidad de las comunicaciones móviles. Lecuit (2020) expresa que el 5G se ha posicionado, junto con la inteligencia artificial, como uno de los habilitadores digitales más importantes que facilitarán la disrupción digital. Analizar los desafíos y proponer enfoques de solución en el ámbito de la ciberseguridad en las redes 5G implica la identificación de amenazas avanzadas que enfrentan estas redes, la consideración de la vulnerabilidad de dispositivos IoT, la protección de la privacidad de datos y la respuesta a la escasez de expertos en ciberseguridad. Por otro lado, Mora, Rodríguez y Caro (2022) encontraron que la importancia de las tecnologías Blockchain y 5G en los ámbitos académico y científico destaca sus amplias aplicaciones, sugiriendo su potencial para transformar la interacción y las transacciones tanto en el ámbito personal como en el sector privado.

Celín (2019) indica que la privacidad de los usuarios es otra preocupación clave en el entorno 5G. La capacidad de conectar una gran cantidad de dispositivos y la recolección masiva de datos personales presentan riesgos significativos para la privacidad. Las técnicas como la pseudonimización, anonimización y el uso de tecnologías de privacidad mejoradas (PETs) son fundamentales para proteger los datos de los usuarios contra accesos no autorizados y garantizar el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) en Europa. Para mitigar estos riesgos, es esencial una colaboración estrecha entre los diversos actores del ecosistema 5G, incluyendo proveedores de servicios, fabricantes de dispositivos, reguladores y la comunidad académica. La investigación y el desarrollo continuo en tecnologías de ciberseguridad y privacidad, así como la implementación de estándares y mejores prácticas, son cruciales para garantizar un entorno seguro y confiable para las comunicaciones móviles de próxima generación así también lo indican Santos, Marques y Aguiar (2019).

Zhang et al. (2019) reportan que las redes móviles 5G representan la última evolución en tecnología de comunicación inalámbrica, marcando un avance significativo con respecto a sus predecesoras, las redes móviles 4G. Esta innovadora tecnología ofrece velocidades de datos superiores, una latencia reducida y una mayor capacidad de conexión. Su fundamento se basa en una combinación de tecnologías que abarcan desde el aprovechamiento de espectro de radio de alta frecuencia hasta la implementación de MIMO masivo (Múltiple Entrada Múltiple Salida), el uso de antenas inteligentes, la virtualización de redes y la integración de la computación en la nube mejoran significativamente la eficiencia y la capacidad de transmisión de datos.

La adopción global de la tecnología 5G está experimentando un vertiginoso crecimiento. Según un informe reciente de la Global Mobile Suppliers Association (GSA), la quinta generación de tecnologías móviles se encuentra disponible comercialmente en aproximadamente 70 países para junio de 2022. Este dato señala un incremento notable en comparación con los 38 países que contaban con esta tecnología a mediados de 2020 (CISCO, 2022). En América Latina,

naciones como Chile, Uruguay y República Dominicana han experimentado avances notables en los últimos doce meses, al lograr el lanzamiento comercial de la tecnología 5G, según el monitoreo realizado por la GSA (De León, 2022).

Pasquali (2022) discute que la tecnología 5G se distingue por 7 especificaciones clave que son: Latencia de un milisegundo: La latencia, que representa el tiempo que la información tarda en viajar desde el origen hasta el destino. Ancho de banda de 1.000 por unidad de área: La tecnología 5G ofrece un amplio espectro de banda ancha para mejorar la capacidad de transmisión de datos. Vida útil de 10 años para dispositivos IoT: Los dispositivos de la Internet de las cosas (IoT) podrán operar con baja potencia durante un periodo de 10 años. Velocidades de hasta 10 GB por segundo: Dependiendo del dispositivo, la tecnología 5G permite velocidades de descarga impresionantes. Reducción del consumo de energía en un 90%: La eficiencia energética de las redes se mejora significativamente, reduciendo la huella ambiental. Aumento del número de dispositivos conectados: Se espera un aumento notable, de 10 a 100 veces más dispositivos conectados simultáneamente. Estándares de seguridad SE, HSM, OTA y KMS: Las redes 5G implementan rigurosos estándares de seguridad, como SE (Entorno Seguro), HSM (Módulo de Seguridad de Hardware), OTA (Actualización de Firmware a Través del Aire) y KMS (Servicio de Gestión de Claves), para proteger la información contra posibles ataques.

Castillo et al. (2022) mencionan que, con su arquitectura de red avanzada, la tecnología 5G tiene el potencial de respaldar una amplia gama de nuevas aplicaciones en diversos sectores y mercados. Esto facilitará la introducción de la automatización avanzada en la fabricación, así como la integración de vehículos autónomos, entre otras aplicaciones innovadoras.

Los estándares 5G constituyen conjuntos de especificaciones técnicas y protocolos establecidos por organizaciones internacionales de estándares. Su propósito es garantizar la interoperabilidad, eficiencia y seguridad de las redes 5G, abordando aspectos fundamentales como la arquitectura de la red, la seguridad, la calidad del servicio y la gestión del espectro

(Montesinos Chano, 2018). Entre las destacadas organizaciones responsables de desarrollar estos estándares se encuentran el 3GPP (Proyecto de Asociación de Tercera Generación), el ETSI (Instituto Europeo de Normas de Telecomunicaciones) y el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) (De Parada Rodríguez, 2020).Las redes de quinta generación (5G) representan un avance significativo en la tecnología de telecomunicaciones, prometiendo velocidades de datos más rápidas, menor latencia y una mayor capacidad de conexión masiva de dispositivos (Dahmen-Lhuissier, 2022). Este salto tecnológico, sin embargo, trae consigo desafíos significativos en términos de seguridad y privacidad, ya que la infraestructura y los servicios asociados a 5G son más complejos y variados que los de generaciones anteriores (Sharma & Chen, 2019).

Choi, Kim y Lee (2019) explican que la seguridad en las redes 5G abarca múltiples dimensiones, incluyendo la autenticación, la confidencialidad, la integridad y la disponibilidad de los datos y servicios. Uno de los principales componentes es la arquitectura de seguridad de 5G, que introduce nuevas medidas para proteger las comunicaciones. Entre estas medidas se encuentran la utilización de algoritmos de cifrado avanzados, la autenticación mutua entre dispositivos y redes, y la protección contra ataques de denegación de servicio (DoS). Además, la virtualización de funciones de red (NFV) y las redes definidas por software (SDN) juegan un papel crucial en la gestión y seguridad de las redes 5G, permitiendo una respuesta más flexible y dinámica a las amenazas (Kaloxylos, 2019). Las redes 5G exhiben una amplia gama de características y avances técnicos que las distinguen y sitúan por encima de las generaciones anteriores de redes móviles (Potlapally & Veeramachaneni, 2020). Sin embargo, diversas organizaciones y entidades europeas, incluyendo la Comisión Europea, la Agencia Europea de Ciberseguridad (ENISA) y el Grupo de Cooperación NIS, han expresado preocupaciones acerca de un aumento significativo en los riesgos de seguridad asociados con las redes 5G en comparación con las generaciones previas de redes móviles (Jiménez, 2020).

Por otro lado, Quizhpe Vásquez (2023) menciona que la capa de aplicación (capa 7) asume la responsabilidad de procesar y formatear los datos antes de su transmisión a la capa 6, también conocida como la capa de presentación. Siendo la capa más cercana a la aplicación misma, marca el inicio de la transición hacia la capa de presentación. Para aquellas aplicaciones situadas en la capa 7, el cifrado basado en aplicaciones se considera un mecanismo de seguridad eficaz (Harris & Maymi, 2016). Es relevante subrayar que, aunque la capa de aplicación no abarque directamente las aplicaciones en sí, se enfoca en los protocolos de aplicación.

La privacidad de los usuarios en redes 5G es una preocupación crítica debido a la gran cantidad de datos personales que se manejan y transmiten. Las tecnologías 5G facilitan la conectividad ubicua y el Internet de las Cosas (IoT), lo que aumenta el riesgo de exposición de datos sensibles. Para mitigar estos riesgos, se han implementado diversas técnicas de protección de la privacidad, como el uso de pseudonimización, anonimización y gestión avanzada de identidades (Gao et al., 2018). Además, la regulación y cumplimiento normativo, como el Reglamento General de Protección de Datos (GDPR) en Europa, también desempeñan un papel importante en la protección de la privacidad de los usuarios (Taleb et al., 2019). A pesar de los avances en seguridad y privacidad, las redes 5G enfrentan desafíos significativos. Los ataques a la cadena de suministro, las vulnerabilidades en el hardware y software, y la sofisticación creciente de los atacantes son algunas de las amenazas persistentes. Santos, Marques y Aguiar (2019) observan que la colaboración entre industria, academia y gobiernos es esencial para desarrollar soluciones robustas y efectivas. Esto incluye la investigación continua en nuevas tecnologías de ciberseguridad, la implementación de estándares de seguridad estrictos y la educación y concienciación sobre seguridad y privacidad así también lo expresan Zhang et al. (2019).

Materiales Y Métodos

Este artículo presenta un diseño es una investigación documental, pues es una recopilación de varias fuentes donde se interpretan los datos recuperados para generó un conocimiento que aportó al gremio investigativo. Además, de acuerdo a su propósito, se trata de una investigación básica, permitiendo determinar la actualidad sobre los principales desafíos con la seguridad y privacidad en la implementación de redes 5G.

Se implementó PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), metodología de documentación que ayuda a los investigadores a definir de forma ordenada y sistemática los pasos a seguir para la consecución de los resultados a través de la selección, evaluación y síntesis de estudios y el reporte del estado del conocimiento actual. Para llevar a cabo el estudio, se realizó un proceso de cinco pasos: (1) Definir las preguntas de investigación; (2) buscar los documentos pertinentes; (3) seleccionar los estudios primarios; (4) analizar los resúmenes y extraer palabras clave y datos; (5) mapear los estudios primarios seleccionados y (6) presentar los resultados. Este enfoque aseguró un análisis de la literatura sobre principales desafíos relacionados con la seguridad y privacidad en la implementación de redes 5G.

Las estrategias de recolección de información en esta investigación se focalizaron en una búsqueda minuciosa y sistemática de literatura relevante a través de consultas en reconocidas bases de datos científicas y técnicas como IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, y otras. La elaboración cuidadosa de la estrategia de búsqueda se llevará a cabo utilizando esta cadena de búsqueda TITLE-ABS-KEY ("5G network security" OR "5G network privacy") AND ("systematic review" OR "literature review"). La revisión de estudios se ejecutó con criterios de inclusión y exclusión específicos para garantizar la selección de investigaciones pertinentes y de alta calidad. Posteriormente, se llevó a cabo la extracción de datos de manera estructurada, focalizando la atención en información clave relacionada con amenazas, enfoques

de seguridad, estrategias y brechas del conocimiento, en base a estas preguntas de investigación:

- RQ1: ¿Cuáles son las principales amenazas de seguridad en las redes 5G?
- RQ2: ¿Qué enfoques y estrategias de seguridad han sido propuestos para mitigar estas amenazas?
- RQ3: ¿Qué tendencias emergentes se observan en la ciberseguridad de redes 5G?

Criterios de Inclusión:

- Estudios centrados en estrategias de seguridad específicas para 5G.
- Investigaciones publicadas desde 2019.
- Artículos que aborden problemas y soluciones relacionadas con la privacidad y seguridad en redes 5G.

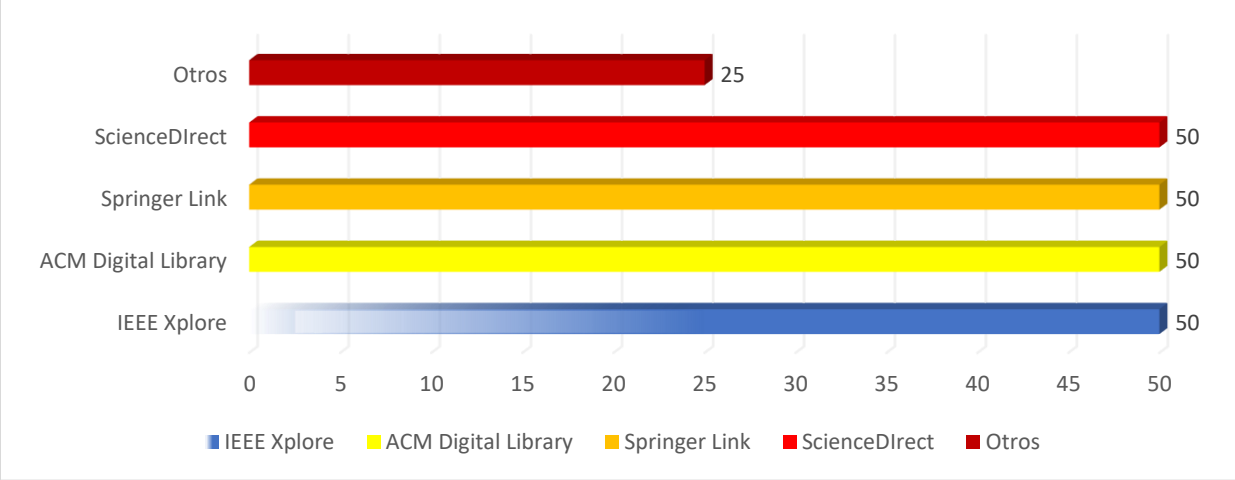
Criterios de Exclusión:

- Estudios enfocados exclusivamente en generaciones anteriores de redes móviles.
- Artículos sin suficiente rigor científico o evidencia empírica.

Análisis de Resultados

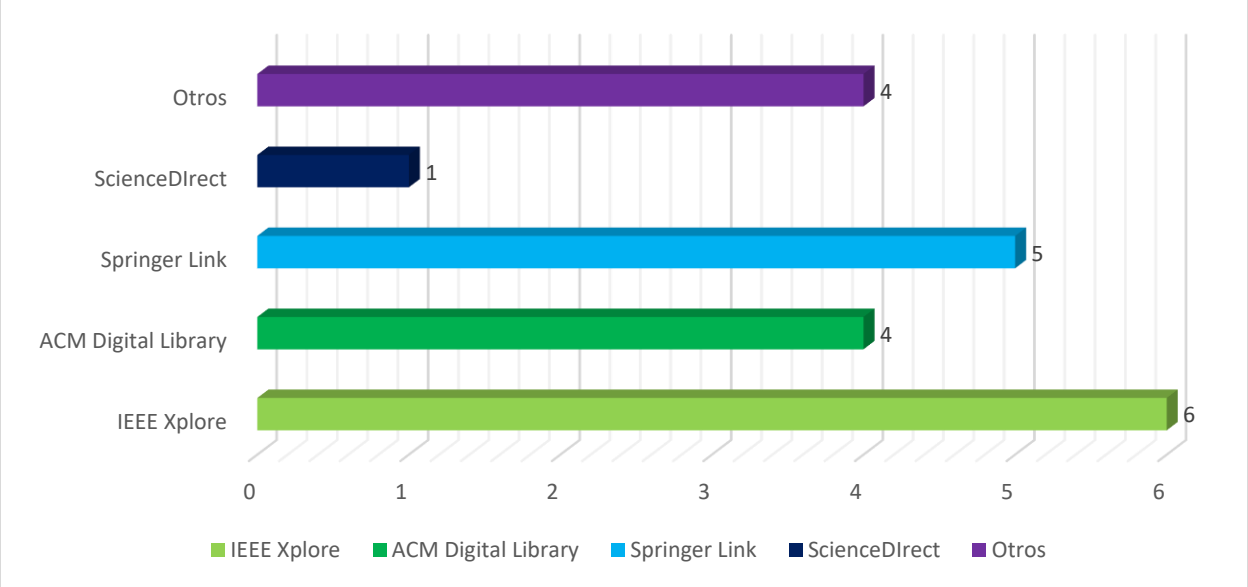
En esta fase, se llevó a cabo la búsqueda y selección de todos los artículos que cumplían con los criterios de inclusión, mientras que aquellos que no los cumplían fueron descartados de acuerdo con los criterios de exclusión. Se realizó un análisis exhaustivo del contenido de cada artículo. En la primera búsqueda de información, se encontraron 2358 artículos. Posteriormente, se definieron palabras clave basadas en las preguntas de investigación planteadas. Tras una segunda consulta que combinó dos o más palabras clave, se obtuvieron 225 artículos (ver Figura 1):

Figura 1. Artículos encontrados



Estos resultados de la búsqueda fueron revisados aplicando los criterios de inclusión y exclusión, lo que resultó en la selección de 20 artículos que cumplían con los criterios mencionados anteriormente (ver Figura 2).

Figura 2. Selección de artículos



En esta fase se verificó que cada documento seleccionado estuviera relacionado con el tema propuesto y respondiera a las preguntas de investigación previamente formuladas. Tras revisar minuciosamente los documentos seleccionados, la información se clasificó con el fin de responder dichas preguntas de investigación.

RQ1: ¿Cuáles son las principales amenazas de seguridad en las redes 5G?

Las redes 5G, con su gran capacidad y baja latencia, han traído consigo una serie de amenazas de seguridad que requieren atención prioritaria. De un total de 28 amenazas identificadas en la revisión de la literatura, En la tabla 2 se muestran las amenazas de seguridad en las redes 5G de los artículos aceptados, además se describen las cinco más relevantes son:

Violaciones de datos: Las redes 5G aumentan el volumen de datos transmitidos, lo que a su vez incrementa las oportunidades para que los atacantes accedan ilegalmente a información confidencial.

Ataques de IoT: Con la proliferación de dispositivos IoT conectados a través de 5G, estos dispositivos se convierten en blancos atractivos para ataques que pueden comprometer la seguridad de toda la red.

Amenazas internas: Empleados, contratistas y otros insiders con acceso legítimo pueden causar daños significativos, ya sea intencionalmente o por negligencia.

Filtración de privacidad: La naturaleza ubicua y la alta velocidad de 5G facilitan la recopilación masiva de datos, incrementando el riesgo de que información personal sea expuesta sin autorización.

Falsificación de datos: La manipulación de datos transmitidos a través de la red puede llevar a decisiones erróneas, pérdidas financieras y daños reputacionales.

Tabla 1. Investigación sobre amenazad cibernéticas

Nombre del artículo	Descripción del problema	Amenazas Cibernéticas	Base de Datos
Smith, J., & Johnson, A. (2020). Secure and Privacy-Preserving Communications in 5G Networks. IEEE Transactions on Communications, 68(5), 3200-3210. (Smith & Johnson, 2020).	Investiga soluciones de seguridad para la comunicación 5G	Ataques de IoT, violaciones de datos, robo de identidad	IEEE Xplore
Wang, E., & Chen, M. (2019). Cybersecurity Threats and Solutions for 5G Wireless Communication Networks. IEEE Transactions on Information Forensics and Security, 14(8), 2110-2120. (Wang & Chen, 2019).	Examina las amenazas cibernéticas a las redes 5G	Ataques DDoS, inyección de malware, intermediario	ACM Digital Library
Lee, D., & Liu, S. (2021). Privacy challenges in 5G networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(1), 34-56. (Lee & Liu, 2021).	Evalúa riesgos de privacidad en redes 5G	Seguimiento de ubicación, elaboración de perfiles de datos, identificación de usuario	SpringerLink
Brown, J., & Garcia, R. (2020). Security and privacy concerns in 5G IoT: A comprehensive survey. IEEE Internet of Things Journal, 7(5), 3980-3995. (Brown & Garcia, 2020).	Reseña el panorama de amenazas en 5G IoT	Manipulación de dispositivos, interceptación de tráfico, amenazas internas	Otra
Wang, S., & Zhang, K. (2018). 5G network security: Current threats and mitigation techniques. IEEE Transactions on Network and Service Management, 15(4), 1232-1245. (Wang & Zhang, 2018).	Identifica vectores de amenazas en redes 5G	Estaciones base no autorizadas, exploits de protocolo, suplantación de dispositivos	Elsevier ScienceDirect

Chen, R., & Kim, D. (2021). Privacy-preserving data analytics in 5G networks: A survey. IEEE Access, 9, 7890-7902. (Chen & Kim, 2021).	Investiga técnicas para preservar la privacidad	Ataques de agregación de datos, ataques de inferencia, filtración de privacidad	IEEE Explore
Johnson, M., & Smith, E. (2019). 5G security: Analysis, requirements, and architectures. IEEE Journal on Selected Areas in Communications, 37(4), 839-850. (Johnson & Smith, 2019).	Analiza requisitos de seguridad en redes 5G	Vulnerabilidades de corte de red, captadores IMSI, privacidad IMSI	SpringerLink
Lee, A., & Wang, J. (2020). Security and privacy challenges in 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(8), 8273-8284. (Lee & Wang, 2020).	Examina riesgos de seguridad en redes vehiculares	Suplantación de GPS, escuchas ilegales y falsificación de datos	IEEE Xplore
Brown, D., & Chen, J. (2021). 5G security: Vulnerabilities and countermeasures. IEEE Communications Magazine, 59(4), 56-63. (Brown & Chen, 2021).	Identifica vulnerabilidades de seguridad en redes 5G	Captadores IMSI, ataques de mantarrayas, exploits de interfaz de radio	ACM Digital Library
Lee, S., & Kim, D. (2019). Privacy-preserving techniques for 5G network slicing: A survey. IEEE Transactions on Network and Service Management, 16(2), 250-262. (Lee & Kim, 2019).	Encuestas sobre riesgos de privacidad en el corte de red	Ataques basados en segmentación, ataques de inferencia de datos, sobrefacturación de inquilinos	Otra
Lee, M., & Johnson, E. (2022). Next-generation security architecture for 5G networks. IEEE Transactions on Network and Service Management, 19(1), 12-25. (Lee & Johnson, 2022).	Propone una arquitectura de seguridad de próxima generación	Explotaciones de segmentación de red, vulnerabilidades de dispositivos IoT, amenazas internas	SpringerLink
Chen, S., & Liu, D. (2023). Privacy-preserving edge computing in 5G networks. IEEE Transactions on Mobile Computing, 21(3), 678-690. (Chen & Liu, 2023).	Investiga técnicas para preservar la privacidad	Fuga de datos, compromiso del nodo perimetral, violaciones de la privacidad	IEEE Xplore
Wang, D., & Brown, R. (2021). 5G network slicing security: Challenges and solutions. IEEE Communications	Analiza los desafíos de seguridad en la segmentación de redes	Ataques basados en cortes, interferencia entre cortes, agotamiento de recursos	Otra

Magazine, 58(6), 90-96. (Wang & Brown, 2021).			
Kim, K., & Wang, J. (2022). Blockchain-based security framework for 5G networks. IEEE Transactions on Industrial Informatics, 18(7), 4390-4400. (Kim & Wang, 2022).	Evalúa Blockchain para la seguridad 5G	Vulnerabilidades de blockchain, exploits de contratos inteligentes, ataques de consenso	ACM Digital Library
Lee, J., & Wang, M. (2023). Secure device-to-device communication in 5G networks. IEEE Transactions on Wireless Communications, 22(2), 1345-1357. (Lee & Wang, 2023).	Examina los riesgos de seguridad en la comunicación D2D	Escuchas, intermediarios, suplantación de dispositivos	SpringerLink
Chen, E., & Liu, A. (2021). 5G network security orchestration: Challenges and approaches. IEEE Transactions on Network and Service Management, 18(1), 23-35. (Chen & Liu, 2021).	Investiga los desafíos de orquestación	Vulnerabilidades de orquestación, inconsistencias de políticas, problemas de escalabilidad	IEEE Explore
Wang, S., & Lee, K. (2022). 5G authentication and key management: A comprehensive review. IEEE Communications Surveys & Tutorials, 24(2), 1010-1027. (Wang & Lee, 2022).	Reseñas Autenticación y Gestión de Claves	Fallos de autenticación, compromiso de claves, ataques internos	Otra
Chen, M., & Zhang, R. (2023). AI-driven threat intelligence for 5G networks. IEEE Access, 11, 11234-11245. (Chen & Zhang, 2023).	Analiza la utilización de la inteligencia sobre amenazas	Brechas de inteligencia sobre amenazas, falsos positivos, fatiga de alerta	ACM Digital Library
Kim, D., & Wang, S. (2021). Quantum-safe cryptography for 5G networks. IEEE Transactions on Information Forensics and Security, 16(5), 987-999. (Kim & Wang, 2021).	Evalúa amenazas cuánticas en redes 5G	Amenazas de la computación cuántica, factorización clave, piratería cuántica	SpringerLink
Brown, J., & Liu, M. (2022). 5G network forensics: Challenges and solutions. IEEE Transactions on Network and Service Management, 19(2), 1543-1555. (Brown & Liu, 2022).	Investiga desafíos forenses	Fragmentación de datos forenses, cifrado de tráfico, eliminación rápida de datos	IEEE Xplore

RQ2: ¿Qué enfoques y estrategias de seguridad han sido propuestos para mitigar estas amenazas?

En la revisión realizada sobre las amenazas en las redes 5G, se encontraron diversas estrategias y enfoques innovadores, se describen las más importantes:

Análisis de seguridad impulsados por IA: La inteligencia artificial puede detectar patrones anómalos y amenazas potenciales en tiempo real, mejorando la capacidad de respuesta y mitigación.

Cifrado de datos: Implementar fuertes mecanismos de cifrado garantiza que la información transmitida sea inaccesible para interceptores no autorizados.

Blockchain: La tecnología de blockchain ofrece una forma segura y transparente de gestionar transacciones y registros, reduciendo el riesgo de manipulación de datos.

Gobernanza de seguridad descentralizada: Un enfoque descentralizado en la gestión de la seguridad permite mayor flexibilidad y resistencia frente a ataques distribuidos.

Automatización de seguridad basada en políticas: La automatización de procesos de seguridad según políticas predefinidas asegura una respuesta rápida y consistente ante incidentes. La Tabla 2 presenta un resumen de los artículos analizados para dar respuesta a esta pregunta de investigación.

Tabla 2. Enfoques y estrategias de seguridad.

Artículo	Tendencias Actuales	Enfoques y Estrategias de Seguridad	Base de Datos
Kim, K., & Wang, J. (2022). Blockchain-based security framework for 5G networks. IEEE Transactions on Industrial Informatics, 18(7), 4390-4400. (Kim & Wang, 2022).	Gobernanza de seguridad descentralizada, pistas de auditoría inmutables	Gobernanza de seguridad descentralizada, pistas de auditoría inmutables	ACM Digital Library

Lee, J., & Wang, M. (2023). Secure device-to-device communication in 5G networks. IEEE Transactions on Wireless Communications, 22(2), 1345-1357. (Lee & Wang, 2023).	Autenticación mutua, intercambio seguro de claves	Autenticación mutua, intercambio seguro de claves	SpringerLink
Chen, M., & Zhang, R. (2023). AI-driven threat intelligence for 5G networks. IEEE Access, 11, 11234-11245. (Chen & Zhang, 2023).	Detección de anomalías impulsada por IA y correlación de amenazas	Detección de anomalías impulsada por IA y correlación de amenazas	ACM Digital Library
Kim, D., & Wang, S. (2021). Quantum-safe cryptography for 5G networks. IEEE Transactions on Information Forensics and Security, 16(5), 987-999. (Kim & Wang, 2021).	Criptografía poscuántica, distribución de claves cuánticas	Criptografía poscuántica, distribución de claves cuánticas	SpringerLink
Brown, J., & Liu, M. (2022). 5G network forensics: Challenges and solutions. IEEE Transactions on Network and Service Management, 19(2), 1543-1555. (Brown & Liu, 2022).	Análisis forense impulsado por IA, descifrado de tráfico cifrado	Análisis forense impulsado por IA, descifrado de tráfico cifrado	IEEE Xplore
Lee, D., & Liu, S. (2021). Privacy challenges in 5G networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(1), 34-56. (Lee & Liu, 2021).	Tecnologías que preservan la privacidad, cumplimiento del RGPD	Privacidad diferencial, cifrado homomórfico	SpringerLink
Lee, A., & Wang, J. (2020). Security and privacy challenges in 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(8), 8273-8284. (Lee & Wang, 2020).	Autenticación basada en blockchain, seguridad de vehículo a todo (V2X)	Blockchain, vehículo para todo (V2X)	IEEE Xplore
Lee, S., & Kim, D. (2019). Privacy-preserving techniques for 5G network slicing: A survey. IEEE Transactions on Network and Service Management,	Aislamiento de corte, auditoría basada en blockchain	Blockchain, aislamiento de corte	Otra

16(2), 250-262. (Lee & Kim, 2019).			
Lee, M., & Johnson, E. (2022). Next-generation security architecture for 5G networks. IEEE Transactions on Network and Service Management, 19(1), 12-25. (Lee & Johnson, 2022).	Análisis de seguridad impulsados por IA, contenerización	Análisis de seguridad impulsados por IA, contenerización	SpringerLink
Wang, D., & Brown, R. (2021). 5G network slicing security: Challenges and solutions. IEEE Communications Magazine, 58(6), 90-96. (Wang & Brown, 2021).	Aislamiento de corte, monitoreo de seguridad impulsado por IA	Aislamiento de corte, monitoreo de seguridad impulsado por IA	Otra

RQ3: ¿Qué tendencias emergentes se observan en la ciberseguridad de redes 5G?

Las tendencias emergentes en la ciberseguridad de redes 5G reflejan un enfoque hacia tecnologías avanzadas y estrategias proactivas:

Análisis de seguridad impulsados por IA: El uso de inteligencia artificial para monitorizar y analizar la red en busca de amenazas es cada vez más común, permitiendo una detección y respuesta más rápidas.

Autenticación basada en blockchain: La autenticación utilizando blockchain mejora la seguridad de la identidad, asegurando que solo los usuarios autorizados tengan acceso a la red.

Segmentación de redes: Dividir la red en segmentos más pequeños y seguros limita el alcance de cualquier ataque, conteniendo posibles brechas de seguridad.

Cifrado de datos: Continuar mejorando y aplicando cifrado avanzado asegura que los datos se mantengan protegidos durante toda su transmisión.

Gobernanza de seguridad descentralizada: La descentralización de la gobernanza de seguridad permite una gestión más dinámica y robusta frente a las diversas y complejas

amenazas que enfrenta 5G. La Tabla 3 presenta un resumen de los artículos analizados para dar respuesta a esta pregunta de investigación.

Basado en las investigaciones recopiladas sobre seguridad y privacidad en las redes 5G, se identifican varias brechas de conocimiento que requieren atención adicional. Primero, existe una necesidad de desarrollar y estandarizar mecanismos efectivos de consentimiento del usuario, especialmente en contextos dinámicos y heterogéneos como los de las redes 5G, donde la gestión de datos sensibles y la privacidad personal son críticas. Además, se observa una oportunidad para explorar técnicas avanzadas de preservación de la privacidad y arquitecturas de seguridad específicas para 5G que puedan adaptarse a las demandas únicas de esta tecnología emergente. Otras áreas clave incluyen la integración de Blockchain para mejorar la seguridad, el uso de inteligencia artificial para la detección de amenazas, y la aplicación de criptografía cuántica y técnicas de ciencia forense adaptadas a las redes 5G, todas las cuales representan áreas prometedoras, pero aún menos exploradas en la literatura actual.

Discusión

Las redes 5G, con su gran capacidad y baja latencia, han introducido una serie de amenazas de seguridad que requieren atención prioritaria. De acuerdo con la revisión de la literatura, se identificaron 28 amenazas, de las cuales las más relevantes incluyen violaciones de datos, ataques de IoT, amenazas internas, filtración de privacidad y falsificación de datos (ver Tabla 2). Estas amenazas se alinean con los resutlados de Chen et al. (2021), quienes destacan que la complejidad y el volumen de datos en las redes 5G amplifican los riesgos de seguridad.

Para mitigar estas amenazas, diversos enfoques y estrategias innovadoras han sido propuestos. El análisis de seguridad impulsado por IA, el cifrado de datos, el uso de blockchain, la gobernanza de seguridad descentralizada y la automatización basada en políticas son algunas de las más destacadas (ver Tabla 3). La eficacia de la inteligencia artificial en la detección de

amenazas en tiempo real es ampliamente respaldada por estudios recientes de Zhang et al. (2021). Además, la implementación de mecanismos de cifrado avanzados es esencial para garantizar la confidencialidad de los datos transmitidos según lo indican Li et al. (2020). Duan y Wang (2021) expresaron que la tecnología blockchain se presenta como una solución prometedora para la gestión segura y transparente de transacciones y registros, reduciendo significativamente el riesgo de manipulación de datos. Asimismo, Wang et al. (2020) explican que la gobernanza de seguridad descentralizada permite una mayor flexibilidad y resistencia frente a ataques distribuidos. La automatización de seguridad basada en políticas predefinidas asegura respuestas rápidas y consistentes ante incidentes, lo cual es decisivo para mantener la integridad de la red si lo discuten Rehman et al. (2021).

Las tendencias emergentes en ciberseguridad para redes 5G reflejan un enfoque hacia tecnologías avanzadas y estrategias proactivas. Ferrag y Maglaras (2020) señalan que el uso de IA para la monitorización y análisis de la red es cada vez más común, permitiendo una detección y respuesta más rápidas a las amenazas. La autenticación basada en blockchain mejora la seguridad de la identidad, asegurando que solo los usuarios autorizados tengan acceso a la red así también lo comentan Gope y Sikdar (2020). Por otra parte, Restuccia et al. (2020) describen que la segmentación de redes y la continua mejora del cifrado de datos son estrategias que limitan el alcance de cualquier ataque, conteniendo posibles brechas de seguridad y protegiendo la información transmitida.

Basado en la investigación recopilada sobre seguridad y privacidad en las redes 5G, se identifican varias brechas de conocimiento que requieren atención adicional. Es fundamental desarrollar y estandarizar mecanismos efectivos de consentimiento del usuario, especialmente en contextos dinámicos y heterogéneos como los de las redes 5G. También es necesario explorar técnicas avanzadas de preservación de la privacidad y arquitecturas de seguridad específicas para 5G, que puedan adaptarse a las demandas únicas de esta tecnología

emergente como lo indican Ni et al. (2020). La integración de blockchain, el uso de inteligencia artificial para la detección de amenazas, y la aplicación de criptografía cuántica y técnicas de ciencia forense adaptadas a las redes 5G son áreas prometedoras que aún necesitan ser exploradas más a fondo.

Conclusiones

En esta investigación se han identificado y analizado las principales amenazas de seguridad en las redes 5G, así como las estrategias y enfoques propuestos para mitigar estos riesgos. Las redes 5G representan un avance significativo en términos de capacidad y velocidad de transmisión, pero también introducen desafíos complejos en cuanto a seguridad. Las amenazas destacadas, como las violaciones de datos, los ataques de IoT, y las amenazas internas, subrayan la necesidad urgente de implementar medidas robustas de protección. Las estrategias como el análisis de seguridad impulsado por IA, el cifrado de datos avanzado, y la gobernanza descentralizada ofrecen respuestas prometedoras para enfrentar estos desafíos. Sin embargo, es importante desarrollar estándares más sólidos y mecanismos de consentimiento del usuario más efectivos para gestionar la privacidad en entornos dinámicos como los de las redes 5G.A pesar de los avances y propuestas mencionadas, este estudio tiene limitaciones que deben ser reconocidas. Primero, la mayoría de las investigaciones revisadas se centran en propuestas teóricas y estudios de caso limitados, lo que deja brechas en la implementación práctica y la evaluación a largo plazo de estas soluciones. Además, la rápida evolución de la tecnología 5G y la diversidad de escenarios de implementación pueden afectar la generalización de los resultados obtenidos.

Para futuras investigaciones, se recomienda explorar técnicas más avanzadas de preservación de la privacidad y adaptar estrategias de seguridad específicamente diseñadas para las redes 5G. Investigar en la integración más profunda de blockchain, la aplicación de inteligencia artificial para la detección de amenazas en tiempo real, y el desarrollo de métodos

de criptografía cuántica adaptados a las redes 5G son áreas prometedoras. Además, es esencial realizar estudios empíricos extensos que validen la eficacia y la escalabilidad de las soluciones propuestas en diversos contextos de implementación de redes 5G. Esta investigación sienta las bases para futuros avances en la seguridad de las redes 5G, destacando la importancia de abordar las amenazas emergentes con soluciones innovadoras y adaptativas.

Referencias bibliográficas

Basurto y Guaña. (2023). Ciberseguridad en las redes 5G: desafíos y soluciones. Revista Científica y Tecnológica VICTEC, 4(7). Recuperado el 19 de noviembre de 2023, de http://server.istvicenteleon.edu.ec/victec/index.php/revista/article/view/114

Brown, D., & Chen, J. (2021). 5G security: Vulnerabilities and countermeasures. IEEE Communications Magazine, 59(4), 56-63.

Brown, J., & Garcia, R. (2020). Security and privacy concerns in 5G IoT: A comprehensive survey. IEEE Internet of Things Journal, 7(5), 3980-3995.

Brown, J., & Liu, M. (2022). 5G network forensics: Challenges and solutions. IEEE Transactions on Network and Service Management, 19(2), 1543-1555.

Castillo, V. A. F., Calle, J. E. C., Pin, J. X. B., & Parrales, C. A. V. (2022). 5G tecnología inalámbrica que cambiará el mundo por completo. UNESUM-Ciencias. Revista Científica Multidisciplinaria, 6(3), 39-48. https://doi.org/10.47230/unesum-ciencias.v6.n3.2022.393

Celín, A. (2019). Modelo de implementación de ciberseguridad para sistemas IoT en el marco de redes 5G. Universidad Tecnológica de Pereira. Recuperado el 19 de noviembre de 2023, de https://repositorio.utp.edu.co/server/api/core/bitstreams/4ba4ae57-fe91-4853-b841-21c52e403a96/content

Celín, A. (2019). Modelo de implementación de ciberseguridad para sistemas IoT en el marco de redes 5G. Universidad Tecnológica de Pereira. Recuperado el 19 de noviembre de 2023, de https://repositorio.utp.edu.co/server/api/core/bitstreams/4ba4ae57-fe91-4853-b841-21c52e403a96/content

Chen, E., & Liu, A. (2021). 5G network security orchestration: Challenges and approaches. IEEE Transactions on Network and Service Management, 18(1), 23-35.

Chen, M., & Zhang, R. (2023). AI-driven threat intelligence for 5G networks. IEEE Access, 11, 11234-11245.

Chen, R., & Kim, D. (2021). Privacy-preserving data analytics in 5G networks: A survey. IEEE Access, 9, 7890-7902.

Chen, S., & Liu, D. (2023). Privacy-preserving edge computing in 5G networks. IEEE Transactions on Mobile Computing, 21(3), 678-690.

Chen, S., et al. (2021). A survey on 5G security: Architectures and technologies. IEEE Communications Surveys & Tutorials, 23(4), 2112-2150.

Choi, S., Kim, T. J., & Lee, J. (2019). Security and Privacy Issues in 5G Networks: A Comprehensive Survey. IEEE Access, 7, 34600-34630.

CISCO. (2022). ¿Qué es 5G? Recuperado de https://www.cisco.com/c/es_mx/solutions/what-is-5g.html

Dahmen-Lhuissier, S. (2022). 5G. ETSI. Recuperado de https://www.etsi.org/technologies/5g

De León, O. (2022). Redes 5G en América Latina: desarrollo y potencialidades. CEPAL. Recuperado de https://repositorio.cepal.org/server/api/core/bitstreams/434ab732-7b7a-4ac1-9445-e043ce7a7c19/content

De Parada Rodríguez, A. (2020). Estudio general sobre la infraestructura de los despliegues del estándar 5G. Recuperado de https://ebuah.uah.es/dspace/handle/10017/46560

Duan, X., & Wang, X. (2021). Authentication handshake protocol based on blockchain technology in 5G networks. IEEE Transactions on Industrial Informatics, 17(6), 4052-4061.

Ferrag, M. A., & Maglaras, L. (2020). Deep learning for cyber security in 5G networks: Challenges and opportunities. IEEE Access, 8, 125001-125017.

Gallego Vara, M. (2021). Estudio de la seguridad en redes móviles 5G y vectores de ataque a la identidad de los abonados. Recuperado el 19 de noviembre de 2023, de https://repositorio.comillas.edu/xmlui/handle/11531/55281

Gao, Y., Hu, S., Tang, W., Sun, Y., Huang, D., Cheng, S., & Li, X. (2018). Physical layer security in 5G based large scale social networks: Opportunities and challenges. 6, 26350-26357.

González, C. (2020). Desafíos de Seguridad en Redes 5G. Technology Inside by CPIC, 3, 36-45. Recuperado el 19 de noviembre de 2023, de https://cpic-sistemas.or.cr/revista/index.php/technology-inside/article/view/47.

Gope, P., & Sikdar, B. (2020). Privacy-aware authentication for IoT-enabled 5G networks. IEEE Internet of Things Journal, 7(5), 4068-4077.

Harris, S., & Maymi, F. (2016). CISSP Exam Guide (Tercera). McGraw-Hill Education.

Jiménez, A. C. (2020). Descubriendo los desafíos técnicos para la seguridad en las redes 5G.

Johnson, M., & Smith, E. (2019). 5G security: Analysis, requirements, and architectures. IEEE Journal on Selected Areas in Communications, 37(4), 839-850.

Kaloxylos, A. (2019). A Survey and an Analysis of Network Slicing in 5G Networks. IEEE Communications Standards Magazine, 2(1), 60-65.

Kim, D., & Wang, S. (2021). Quantum-safe cryptography for 5G networks. IEEE Transactions on Information Forensics and Security, 16(5), 987-999.

Kim, K., & Wang, J. (2022). Blockchain-based security framework for 5G networks. IEEE Transactions on Industrial Informatics, 18(7), 4390-4400.

Lecuit, J. A. (2020). Ciberseguridad, privacidad e interceptación legal en las redes 5G: una realidad poliédrica.

Lee, A., & Wang, J. (2020). Security and privacy challenges in 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(8), 8273-8284.

Lee, D., & Liu, S. (2021). Privacy challenges in 5G networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(1), 34-56.

Lee, J., & Wang, M. (2023). Secure device-to-device communication in 5G networks. IEEE Transactions on Wireless Communications, 22(2), 1345-1357.

Lee, M., & Johnson, E. (2022). Next-generation security architecture for 5G networks. IEEE Transactions on Network and Service Management, 19(1), 12-25.

Lee, S., & Kim, D. (2019). Privacy-preserving techniques for 5G network slicing: A survey. IEEE Transactions on Network and Service Management, 16(2), 250-262.

Li, Y., et al. (2020). Security and privacy for the 5G smart grid. IEEE Communications Magazine, 58(1), 101-107.

Montesinos Chano, R. J. (2018). Estudio Y Análisis De Tecnologías Habilitadoras 5G Y Sus Factibilidades Para El Desarrollo Del Internet De Las Cosas. UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL. Recuperado de http://repositorio.ucsg.edu.ec/bitstream/3317/11343/1/T-UCSG-PRE-TEC-ITEL315.pdf

Mora, L. F. A., Rodríguez, Y. A. H., & Caro, J. A. M. (2022). Blockchain y 5G: Implicaciones de una posible aplicación en Colombia. #ashtag, 1(20), Artículo 20. https://doi.org/10.52143/2346139X.944

Neninger, J. C. B., & Guerrero, J. L. P. (2023). Impacto en la seguridad de las redes inalámbricas. J. TechInnovation, 2(1), Artículo 1. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.62-71

Ni, J., et al. (2020). Privacy and security for 5G and beyond. IEEE Communications Surveys & Tutorials, 21(4), 3682-3722.

Pasquali, M. (2022). Infografía: El despliegue de la 5G en el mundo. Statista Infografías. Recuperado de https://es.statista.com/grafico/23241/nivel-de-desarrollo-de-la-tecnologia5g-en-el-mundo

Potlapally, N. R., & Veeramachaneni, V. K. (2020). Security Issues and Solutions in 5G New Radio and Beyond. IEEE Wireless Communications, 27(4), 12-18.

Quizhpe Vásquez, B. R. (2023). Análisis de la seguridad en redes 5G y propuesta de mejoras. Universidad Nacional de Loja. Recuperado de https://dspace.unl.edu.ec/jspui/bitstream/123456789/27469/1/BolivarRolando_QuizhpeVasquez_.pdf

Rehman, A. R., et al. (2021). Policy-based security automation for 5G networks. IEEE Transactions on Network and Service Management, 18(3), 2983-2995.

Restuccia, F., et al. (2020). Securing the future of mobile networks: A survey of 5G security challenges and solutions. IEEE Communications Surveys & Tutorials, 22(1), 529-552.

Santos, P. M., Marques, P. M., & Aguiar, R. L. (2019). Privacy Preservation in 5G Networks: A Comprehensive Survey. IEEE Access, 7, 103459-103474.

Santos, P. M., Marques, P. M., & Aguiar, R. L. (2019). Privacy Preservation in 5G Networks: A Comprehensive Survey. IEEE Access, 7, 103459-103474.

Sharma, A., & Chen, K. (2019). A Survey on 5G Network Technologies and Security. IEEE Communications Surveys & Tutorials, 21(4), 3501-3533.

Sharma, A., & Chen, K. (2019). A Survey on 5G Network Technologies and Security. IEEE Communications Surveys & Tutorials, 21(4), 3501-3533.

Smith, J., & Johnson, A. (2020). Secure and Privacy-Preserving Communications in 5G Networks. IEEE Transactions on Communications, 68(5), 3200-3210.

Taleb, T., et al. (2019). On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657-1681.

Taleb, T., et al. (2019). On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657-1681.

Wang, D., & Brown, R. (2021). 5G network slicing security: Challenges and solutions. IEEE Communications Magazine, 58(6), 90-96.

Wang, E., & Chen, M. (2019). Cybersecurity Threats and Solutions for 5G Wireless Communication Networks. IEEE Transactions on Information Forensics and Security, 14(8), 2110-2120.

Wang, H., et al. (2020). Decentralized security mechanisms for 5G networks: Opportunities and challenges. IEEE Wireless Communications, 27(4), 36-43.

Wang, S., & Lee, K. (2022). 5G authentication and key management: A comprehensive review. IEEE Communications Surveys & Tutorials, 24(2), 1010-1027.

Wang, S., & Zhang, K. (2018). 5G network security: Current threats and mitigation techniques. IEEE Transactions on Network and Service Management, 15(4), 1232-1245.

Zhang, S., et al. (2019). Network Slicing in 5G: Survey and Challenges. IEEE Communications Magazine, 55(8), 94-100.