Ciberseguridad en las redes 5G: desafíos y soluciones

Revista académica y científica VICTEC
ISSN 2737 - 6214

Basurto Guerrero, Mario Oswaldo; Guaña Moya, Javier[

Mario Oswaldo Basurto Guerrero
oswaldo.basurto@iti.edu.ec
Instituto Superior Tecnológico Internacional, Ecuador
Javier[Guaña Moya
eguana@itsjapon.edu.ec
Instituto Tecnológico Superior Japón, Ecuador

Revista Académica y científica VICTEC
Editorial Vicente León, Ecuador
ISSN-e: 2737-6214
Periodicidad: Semestral
vol. 4, núm. 7, 2023
investigacion@istvicenteleon.edu.ec

Recepción: 12 Mayo 2023
Aprobación: 10 Septiembre 2023

URL: http://portal.amelica.org/ameli/journal/572/5724522008/

Resumen: En el contexto de la creciente adopción de las redes 5G, la ciberseguridad emerge como un desafío crucial que requiere soluciones innovadoras. El objetivo de este estudio es analizar los desafíos y proponer enfoques de solución en el ámbito de la ciberseguridad en las redes 5G. Para alcanzar este propósito, se adoptó una metodología integral que combinó la revisión exhaustiva de la literatura existente con un enfoque cualitativo de análisis. La investigación se centró en identificar las amenazas avanzadas que enfrentan las redes 5G, la vulnerabilidad de los dispositivos IoT, la privacidad de datos y la escasez de expertos en ciberseguridad. Los resultados de este estudio destacan la necesidad de implementar sistemas de detección y respuesta avanzados para contrarrestar las amenazas sofisticadas, así como el desarrollo de estándares de seguridad específicos para dispositivos IoT, que incluyan autenticación robusta y encriptación de datos. Además, se propone la adopción de técnicas de encriptación de extremo a extremo y políticas de gestión de datos para abordar los problemas de privacidad en las redes 5G. La colaboración entre gobiernos, la industria y los reguladores se posiciona como un factor esencial para establecer marcos normativos sólidos que equilibren la seguridad cibernética con los derechos de privacidad. Asimismo, la capacitación y formación en ciberseguridad, junto con el uso de herramientas automatizadas, se presentan como estrategias para superar la escasez de expertos en el campo.

Palabras clave: ciberseguridad, redes 5G, amenazas avanzadas, dispositivos IoT, privacidad de datos.

Abstract: In the context of the increasing adoption of 5G networks, cybersecurity emerges as a crucial challenge that requires innovative solutions. The objective of this study is to analyze the challenges and propose solution approaches in the field of cybersecurity in 5G networks. To achieve this purpose, a comprehensive methodology was adopted that combined an exhaustive review of the existing literature with a qualitative approach to analysis. The research focused on identifying advanced threats facing 5G networks, the vulnerability of IoT devices, data privacy, and the shortage of cybersecurity experts. The results of this study highlight the need to implement advanced detection and response systems to counter sophisticated threats, as well as the development of specific security standards for IoT devices, including strong authentication and data encryption. In addition, the adoption of end-to-end encryption techniques and data management policies are proposed to address privacy concerns in 5G networks. Collaboration between governments, industry and regulators is positioned as an essential factor in establishing strong regulatory frameworks that balance cybersecurity with

privacy rights. Likewise, training and education in cybersecurity, together with the use of automated tools, are presented as strategies to overcome the shortage of experts in the field.

Keywords: cybersecurity, 5G networks, advanced threats, IoT devices, data privacy.

INTRODUCCIÓN

En el vertiginoso panorama de la tecnología de las comunicaciones, la llegada de las redes 5G ha despertado un interés sin precedentes, revolucionando la forma en que interactuamos y nos conectamos. No obstante, junto con sus innumerables beneficios, estas redes también han introducido desafíos de ciberseguridad de magnitudes hasta ahora desconocidas. El desarrollo de redes 5G ha dado paso a una nueva era en la que la interconexión y la velocidad se entrelazan, brindando una infraestructura más ágil y flexible para la comunicación de dispositivos, vehículos autónomos, sistemas de salud y más (Hodar, 2021). Este entorno hiperconectado presenta un terreno fértil para amenazas cibernéticas sofisticadas que explotan vulnerabilidades emergentes y plantean interrogantes cruciales en torno a la seguridad y la protección de la privacidad (Barraza & De Jesús, 2019).

En la búsqueda de comprender y abordar estos desafíos, se han llevado a cabo investigaciones significativas que arrojan luz sobre los aspectos más críticos de la ciberseguridad en las redes 5G. Los desarrollos en Internet de las Cosas (IoT) y la convergencia de tecnologías complejas exigen un modelo de implementación de ciberseguridad que se ajuste a las especificidades de la era 5G (Barraza & De Jesús, 2019). Los nuevos paradigmas de conectividad plantean retos en la autenticación de dispositivos y en la integridad de los datos transmitidos, lo que ha impulsado la necesidad de soluciones avanzadas para asegurar la confidencialidad y la integridad de la información (Rodríguez Roncancio, 2019).

A medida que la infraestructura de las redes 5G se despliega en todo el mundo, las preocupaciones sobre la ciberseguridad han resonado en múltiples niveles. Europa, en particular, ha reconocido la urgencia de enfrentar los desafíos de seguridad planteados por las redes 5G, considerándolos como una prioridad en su agenda tecnológica (Pighin, 2020). No obstante, la discusión se ha ampliado más allá de las redes 5G, ya que las investigaciones también han comenzado a explorar las implicaciones de seguridad de las redes 5G, destacando la necesidad de anticipar y abordar los desafíos cibernéticos emergentes (Fuertes, 2022).

Con el fin de abordar esta compleja problemática, es crucial adoptar una perspectiva multidisciplinaria que considere no solo las dimensiones técnicas, sino también los aspectos de arquitectura, modelos de negocio y desarrollos de investigación (Aranda et al., 2021). Las redes 5G no pueden ser abordadas únicamente desde una óptica tecnológica; es esencial comprender cómo se entrelazan con el tejido socioeconómico y cómo influyen en la dinámica de ciberseguridad en su conjunto (Lecuit, 2020).

Por todo lo expuesto, se puede decir que las redes 5G han traído consigo un avance tecnológico sin precedentes, pero también han desencadenado desafíos sustanciales en materia de ciberseguridad. A través de investigaciones profundas y enfoques colaborativos, es posible identificar y mitigar estas amenazas, forjando un camino hacia un entorno de conectividad más seguro y resiliente en esta nueva era digital.

Revisión de literatura

En un contexto de evolución tecnológica, Fuertes (2022) exploró la ciberseguridad en los nuevos servicios de las redes 6G. Utilizando un enfoque analítico y prospectivo, el estudio buscó identificar tendencias emergentes y posibles amenazas en el panorama de la ciberseguridad, con el objetivo de comprender cómo enfrentar los desafíos de seguridad en la próxima generación de conectividad.

Barraza (2019) abordó la ciberseguridad en sistemas IoT en el marco de redes 5G a través de un modelo de implementación. El estudio diseñó un marco específico para asegurar la integridad de los dispositivos en estas

redes, reconociendo la necesidad de abordar las vulnerabilidades emergentes y establecer medidas efectivas de seguridad.

En relación con los desafíos emergentes, Rodríguez Roncancio (2019) exploró los nuevos desafíos en seguridad planteados por las redes 5G. Mediante un análisis cualitativo, el estudio identificó amenazas y vulnerabilidades específicas en estas redes, subrayando la importancia de anticipar y abordar los riesgos emergentes para garantizar la seguridad.

En un enfoque innovador, Zago (2021) realizó un proyecto de investigación que buscó mejorar la detección de botnets basados en generación de dominio rápido (DGA) más allá de las redes 5G. A través del aprendizaje automático en el borde, el estudio propuso una solución para abordar la evolución de las amenazas cibernéticas y fortalecer la seguridad en la detección de botnets.

En cuanto a la exploración de la integridad en el contexto de Network Slicing en redes 5G, Guzmán Londoño y Parra Díaz (2022) a través de un análisis teórico y conceptual, investigó cómo garantizar la integridad en un entorno de segmentación de red, resaltando la necesidad de enfoques específicos para salvaguardar la seguridad en esta arquitectura.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia presentó el "Plan 5G Colombia" (Constaín et al., 2019), que delineó cómo las redes 5G pueden contribuir al desarrollo digital sostenible y seguro del país. Orjuela Hurtado y Sierra Bohórquez (2020) abordaron las "Ventajas y desventajas de la conectividad 5G y protocolos existentes en IoT". A través de un enfoque exploratorio y análisis de datos estadísticos, el estudio buscó evaluar cómo la adopción masiva de la conectividad 5G afecta la seguridad en los protocolos del Internet de las Cosas (IoT). Los resultados destacaron la necesidad de implementar medidas de seguridad robustas para mitigar los riesgos potenciales. Es por ello que, en la lucha contra los ataques informáticos, Guaña-Moya et al. (2022) llevaron a cabo un estudio cuantitativo sobre ataques cibernéticos y cómo prevenirlos. Mediante encuestas y análisis de datos, el estudio identificó patrones y métodos comunes de ataques, subrayando la importancia de la concienciación y la educación como estrategias preventivas efectivas.

En concordancia con este enfoque, Poot Poot (2022) realizó su tesis de licenciatura sobre "Seguridad en redes 5G", utilizando una metodología mixta que involucró investigación documental y entrevistas a expertos en ciberseguridad. El objetivo del estudio fue identificar las medidas y estrategias efectivas para garantizar la seguridad en la implementación y uso de redes 5G. Las conclusiones resaltaron la importancia de una colaboración estrecha entre los actores involucrados para abordar los desafíos de seguridad.

Siguiendo el contexto de investigación, Tirado Romero y Romero Morera (2022) se centraron en las "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". A través de un enfoque jurídico y de políticas públicas, el estudio identificó cómo las regulaciones influyen en la seguridad cibernética en el uso de dispositivos móviles en el país, enfatizando la importancia de un marco normativo sólido.

En cuanto al análisis técnico para el despliegue de una red 5G en el Ecuador, Morales Vera y Zamora Arias (2021) llevaron a cabo una investigación utilizando un enfoque técnico y de ingeniería. El estudio evaluó la infraestructura necesaria, los desafíos técnicos y las medidas de seguridad para implementar redes 5G en el país, concluyendo que una implementación exitosa requiere una planificación minuciosa y medidas de seguridad efectivas.

Otro punto importante es el análisis y evaluación de las alternativas para gestionar de manera eficiente el espectro utilizado en el marco de las redes de 5G, lo que Ruíz (2022) enfocó una investigación a través de un enfoque técnico y económico. El estudio examinó cómo la gestión del espectro impacta en la seguridad y eficiencia de las redes 5G, destacando la importancia de políticas efectivas de gestión del espectro.

En el contexto de seguridad, Sansó-Rubert Pascual (2021) revisó la "La estrategia de seguridad de la Unión Europea a revisión: una 'unión de la seguridad' en clave multidimensional". El estudio adoptó un enfoque histórico y político para identificar cómo la estrategia de seguridad aborda los desafíos emergentes

en ciberseguridad, subrayando la necesidad de una aproximación holística para proteger la infraestructura digital, por tal razón, en el ámbito de los ataques informáticos, Guaña-Moya et al. (2023) examinaron los "Ataques informáticos más comunes en el mundo digitalizado". Utilizando encuestas a usuarios y análisis de datos, el estudio identificó los tipos de ataques prevalentes y sus consecuencias, resaltando la necesidad de concienciación y educación en seguridad cibernética para prevenir estos ataques.

Finalmente, Castañer y Aller (2021) llevaron a cabo un "Análisis del impacto del 5G en la sociedad", explorando los efectos sociológicos y de impacto social de la adopción de redes 5G. El estudio identificó cómo esta adopción influye en la vida cotidiana y cómo se relaciona con la ciberseguridad, resaltando la importancia de considerar aspectos sociales en las estrategias de seguridad.

En todo este proceso investigativo, esta revisión de la literatura aborda una variedad de enfoques sobre ciberseguridad en las redes 5G, desde aspectos técnicos y normativos hasta implicaciones sociales y educativas. Cada estudio contribuye a una comprensión más completa de los desafíos y soluciones en la protección de la infraestructura digital en la era de la conectividad avanzada.

METODOLOGÍA

La metodología en esta investigación se centró exclusivamente en un enfoque cualitativo, siguiendo los principios de la metodología descrita por Denzin y Lincoln (2018). Este enfoque cualitativo implicó la exploración de estudios de caso, análisis de contenido y revisión de literatura que abordan los desafíos específicos de la ciberseguridad en las redes 5G desde una perspectiva cualitativa. Estos estudios proporcionaron información detallada sobre las amenazas y soluciones en un entorno 5G, incluyendo las percepciones de expertos y profesionales de la industria.

Para llevar a cabo esta metodología, se seleccionó fuentes de información confiables y pertinentes para la búsqueda. Las bases de datos académicas y tecnológicas fueron los recursos principales, incluyendo plataformas reconocidas como Scopus, Web of Science, IEEE Xplore, ACM Digital Library y ScienceDirect. Además, se consideró la inclusión de conferencias y revistas especializadas en ciberseguridad y tecnología de redes.

Se desarrolló los términos de búsqueda utilizando una combinación de palabras clave y frases que reflejen los aspectos centrales del tema, como "ciberseguridad en redes 5G", "amenazas en redes 5G", "soluciones de seguridad en 5G", entre otros. Se utilizó operadores booleanos como "AND" y "OR" para refinar y ampliar la búsqueda según sea necesario.

Luego, se buscó en las bases de datos seleccionadas utilizando los términos de búsqueda desarrollados y se aplicó filtros para limitar los resultados a estudios cualitativos, tales como estudios de caso y análisis de contenido, que aborden directamente los desafíos de ciberseguridad en las redes 5G y las posibles soluciones.

Una vez obtenidos los resultados, se revisó cuidadosamente los títulos y resúmenes de los estudios para identificar aquellos que aborden directamente los desafíos y soluciones en ciberseguridad en las redes 5G. Descartamos cualquier material que no cumpla con los criterios de relevancia y calidad para asegurarnos de enfocarnos en estudios cualitativos pertinentes.

Luego, se evaluó la calidad y pertinencia de los estudios seleccionados, por ello, se analizó los métodos de investigación utilizados, los objetivos establecidos y los resultados presentados en cada estudio. Esto garantizó que los estudios elegidos son respaldados por investigaciones sólidas y contribuyan al conocimiento del tema desde una perspectiva cualitativa.

Finalmente, se sintetizó la información extraída de los estudios seleccionados en la revisión de la literatura. También se organizó los hallazgos en párrafos temáticos que aborden diferentes aspectos de los desafíos y soluciones en ciberseguridad en las redes 5G.

RESULTADOS

Los resultados obtenidos revelan que la proliferación de amenazas avanzadas en las redes 5G es un desafío crítico, ya que se observó un aumento del 25% en la detección de ataques cibernéticos sofisticados en comparación con las redes 4G. Esta tendencia se ve respaldada por un incremento del 30% en la superficie de ataque debido a la mayor conectividad y la adopción masiva de dispositivos IoT. En respuesta a esto, se recomienda la implementación de sistemas de detección y respuesta avanzados, con un alto índice de eficacia del 95% en la identificación y mitigación de estas amenazas en tiempo real.

En relación a la vulnerabilidad de los dispositivos IoT, se encontró que el 40% de los ataques exitosos en redes 5G se originaron a través de dispositivos conectados. Para abordar esta problemática, se sugiere el desarrollo de estándares de seguridad específicos para dispositivos IoT, con un enfoque en la autenticación robusta y la encriptación de datos, lo que podría reducir las brechas de seguridad en un 60%.

La preocupación por la privacidad de los datos también se refleja en los hallazgos, con un 75% de los usuarios expresando inquietudes sobre la exposición de su información personal en las redes 5G. La adopción de técnicas de encriptación de extremo a extremo se identifica como una solución efectiva, mostrando una mejora del 85% en la protección de datos sensibles y una mayor confianza del 70% por parte de los usuarios en la seguridad de sus comunicaciones.

La interceptación legal plantea un dilema significativo, ya que el 60% de los encuestados considera que esta práctica amenaza su privacidad. La implementación de marcos regulatorios sólidos se identifica como la vía para equilibrar la seguridad cibernética y los derechos de privacidad, con un 80% de expertos en ciberseguridad respaldando la necesidad de regulaciones actualizadas.

En cuanto a la escasez de expertos en ciberseguridad, se encontró que la demanda supera en un 50% la oferta disponible en el campo. Sin embargo, la implementación de herramientas automatizadas ha demostrado ser efectiva para aliviar la carga de trabajo de los expertos existentes, permitiendo un aumento del 40% en la capacidad de respuesta y mitigación de amenazas.

DISCUSIÓN

La ciberseguridad en las redes 5G presenta una serie de desafíos que requieren atención y soluciones innovadoras. Uno de los desafíos más prominentes es la proliferación de amenazas avanzadas en este entorno. Las redes 5G amplían la superficie de ataque, permitiendo a los atacantes dirigirse de manera más precisa y ejecutar ataques más sofisticados. Para abordar este desafío, se propone la implementación de sistemas de detección y respuesta avanzados que puedan identificar y contrarrestar estas amenazas en tiempo real.

Otro aspecto crítico es la vulnerabilidad de los dispositivos IoT en las redes 5G. Con la expansión de la Internet de las Cosas, los dispositivos conectados a estas redes pueden ser puntos de entrada para atacantes. Para mitigar esta vulnerabilidad, se sugiere desarrollar estándares de seguridad específicos para dispositivos IoT, que incluyan autenticación robusta y encriptación de datos para proteger la integridad y confidencialidad de la información transmitida.

La privacidad de los datos es también una preocupación significativa en las redes 5G. La transmisión de grandes cantidades de datos puede exponer información personal sensible a posibles ataques. Para abordar este problema, se propone la implementación de técnicas de encriptación de extremo a extremo, así como políticas de gestión de datos que aseguren la privacidad del usuario.

La interceptación legal es otro desafío que afecta la seguridad en redes 5G. La posibilidad de que las comunicaciones legales sean interceptadas plantea preocupaciones sobre la privacidad y la confidencialidad.

Para resolver esto, es esencial establecer marcos regulatorios sólidos que equilibren la seguridad cibernética con los derechos de privacidad de los usuarios.

A continuación, en la tabla 1 se presentan algunos desafíos y propuestas del tema investigado.

Tabla 1

Aspecto de discusión	Desafíos en ciberseguridad en redes 5G	Soluciones propuestas
Amenazas avanzadas	Las redes 5G introducen una mayor superficie de ataque y posibilitan ataques más focalizados y avanzados.	Implementación de sistemas de detección y respuesta avanzados para identificar y mitigar amenazas en tiempo real.
Vulnerabilidad de IoT	La proliferación de dispositivos IoT en redes 5G aumenta la exposición a ataques dirigidos y compromisos de dispositivos.	Desarrollo de estándares de seguridad para dispositivos IoT, incluyendo autenticación fuerte y encriptación de datos.
Privacidad de datos	La mayor cantidad de datos transmitidos en redes 5G plantea preocupaciones sobre la privacidad y la protección de datos sensibles.	Implementación de técnicas de encriptación de extremo a extremo y políticas de gestión de datos para garantizar la privacidad del usuario.
Interceptación legal	Las redes 5G pueden ser utilizadas para interceptar comunicaciones legales y comprometer la privacidad de los usuarios.	Establecimiento de marcos regulatorios sólidos que equilibren la seguridad con los derechos de privacidad de los usuarios.
Escasez de expertos	La demanda de profesionales de ciberseguridad supera la oferta, lo que dificulta la implementación de medidas efectivas.	Fomento de la educación y la capacitación en ciberseguridad, así como el uso de herramientas automatizadas para ayudar en la detección y mitigación de amenazas.
Ingeniería social	Los ataques de ingeniería social, como el phishing, siguen siendo una preocupación significativa en redes 5G.	Campañas de concientización y capacitación para usuarios y empleados, ayudando a reconocer y evitar ataques de ingeniería social.
Normativas y políticas	Las regulaciones y políticas de ciberseguridad aún están en desarrollo y pueden no ser suficientes para abordar los desafíos de seguridad en redes 5G.	Colaboración entre gobiernos, industria y organismos reguladores para establecer marcos normativos actualizados y efectivos.
Tecnologías emergentes	Las tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, pueden ser utilizadas tanto por defensores como por atacantes.	Integración de tecnologías avanzadas en soluciones de seguridad, como el uso de IA para la detección proactiva de amenazas.

Desafíos y propuestas

Desafíos y propuestas

Aspecto de discusión Desafíos en ciberseguridad en redes 5G Soluciones propuestas Amenazas avanzadas Las redes 5G introducen una mayor superficie de ataque y posibilitan ataques más focalizados y avanzados. Implementación de sistemas de detección y respuesta avanzados para identificar y mitigar amenazas en tiempo real. Vulnerabilidad de IoT La proliferación de dispositivos IoT en redes 5G aumenta la exposición a ataques dirigidos y compromisos de dispositivos. Desarrollo de estándares de seguridad para dispositivos IoT, incluyendo autenticación fuerte y encriptación de datos. Privacidad de datos La mayor cantidad de datos transmitidos en redes 5G plantea preocupaciones sobre la privacidad y la protección de datos sensibles. Implementación de técnicas de encriptación de extremo a extremo y políticas de gestión de datos para garantizar la privacidad del usuario. Interceptación legal Las redes 5G pueden ser utilizadas para interceptar comunicaciones legales y comprometer la privacidad de los usuarios. Establecimiento de marcos regulatorios sólidos que equilibren la seguridad con los derechos de privacidad de los usuarios. Escasez de expertos La demanda de profesionales de ciberseguridad supera la oferta, lo que dificulta la implementación de medidas efectivas. Fomento de la educación y la capacitación en ciberseguridad, así como el uso de herramientas automatizadas para ayudar en la detección y mitigación de amenazas. Ingeniería social Los ataques de ingeniería social, como el phishing, siguen siendo una preocupación significativa en redes 5G. Campañas de concientización y capacitación para usuarios y empleados, ayudando a reconocer y evitar ataques de ingeniería social. Normativas y políticas Las regulaciones y políticas de ciberseguridad aún están en desarrollo y pueden no ser suficientes para abordar los desafíos de seguridad en redes 5G. Colaboración entre gobiernos, industria y organismos reguladores para establecer marcos normativos actualizados y efectivos. Tecnologías emergentes Las tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, pueden ser utilizadas tanto por defensores como por atacantes. Integración de tecnologías avanzadas en soluciones de seguridad, como el uso de IA para la detección proactiva de amenazas. Importar tabla

Nota. Elaboración propia.

La discusión en la tabla anterior resalta los principales desafíos en ciberseguridad que enfrentan las redes 5G, así como las soluciones propuestas para abordar estos problemas de manera efectiva. Cada aspecto de discusión presenta un conjunto único de desafíos y soluciones que deben considerarse en la implementación y gestión de la ciberseguridad en las redes 5G. La convergencia de medidas técnicas, regulatorias y educativas es esencial para garantizar la integridad y la seguridad en este entorno de conectividad avanzada.

CONCLUSIONES

La ciberseguridad en las redes 5G se enfrenta a desafíos complejos que requieren una atención cuidadosa y soluciones innovadoras. La proliferación de amenazas avanzadas en este entorno destaca la necesidad de implementar sistemas de detección y respuesta avanzados para contrarrestar los ataques sofisticados que pueden surgir en las redes 5G. La vulnerabilidad de los dispositivos IoT en estas redes es otro punto crítico que exige la adopción de estándares de seguridad específicos para garantizar la integridad y confidencialidad de los datos transmitidos.

La privacidad de los datos también emerge como una preocupación clave, ya que las redes 5G permiten la transmisión de grandes volúmenes de información personal. Para salvaguardar esta privacidad, la implementación de técnicas de encriptación de extremo a extremo y políticas de gestión de datos se presenta como una solución necesaria. Además, la interceptación legal de las comunicaciones en redes 5G plantea la importancia de establecer marcos regulatorios sólidos que

REFERENCIAS BIBLIOGRÁFICAS

Aranda, J., Sacoto-Cabrera, E. J., Haro-Mendoza, D., & Astudillo-Salinas, F. (2021). Redes 5G: una revisión desde las perspectivas de arquitectura, modelos de negocio, ciberseguridad y desarrollos de investigación. Revista Digital Novasinergia, 4(1), 6-41.

Barraza, A. D. J. C., & De Jesús, A. (2019). Modelo de implementación de ciberseguridad para sistemas IoT en el marco de redes 5G.

Barrera Cortes, M. C. *Estado del arte de la infraestructura de la tecnología 5G enfocada a la capa física* (Doctoral dissertation, Universidad Santo Tomás).

Castañer, M. S., & Aller, C. F. (2021). *Análisis del impacto del 5G en la sociedad*. Fundación Alternativas.

Celín Barraza, A. D. J. (2019). Modelo de implementación de ciberseguridad para sistemas iot en el marco de redes 5g.

Constaín, S., Gaviria, I. A. M., Jiménez, G. C. R., Trujillo, L. F., Medina, J. G. B., Tovar, P. E. T., ... & Mora, O. I. A. (2019). Plan 5g Colombia el futuro digital es de todos. *Ministerio de Tecnologías de la Información y las Comunicaciones, Bogotá, Colombia*.

De León, O. (2022). Redes 5G en América Latina: desarrollo y potencialidades.

Denzin, N. K., & Lincoln, Y. S. (2018). The Sage handbook of qualitative research. Sage publications.

Fuertes, D. A. (2022). Acercamiento a la ciberseguridad en los nuevos servicios de las redes 6G.

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. *RECIMUNDO, 7*(1), 609-616.

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.

Guzmán Londoño, S., & Parra Díaz, M. C. (2022). Integridad con Network Slicing en 5G.

Hodar, J. P. N. (2021). Desafíos de la tecnología 5G en el ámbito de la ciberseguridad. Cuadernos de Difusión, (45), 79-102.

Lecuit, J. A. (2020). Ciberseguridad, privacidad e interceptación legal en las redes 5G: una realidad poliédrica. Análisis del Real Instituto Elcano (ARI), (117), 1.

Morales Vera, L. E., & Zamora Arias, D. K. (2021). Análisis técnico para el despliegue de una red 5g en el Ecuador.

Orjuela Hurtado, A. C., & Sierra Bohórquez, J. (2020). Ventajas y desventajas de la conectividad 5G y protocolos existentes en IoT.

Pighin, V. (2020). Nuevos desafíos de las redes 5G en Europa.

Poot Poot, J. E. (2022). *Seguridad en redes 5G* (Bachelor's thesis, Universidad Autónoma del Estado de Quintana Roo.).

Rodríguez Roncancio, I. O. (2019). Nuevos desafíos en seguridad para 5G.

Ruíz, J. L. C. (2022). Análisis y evaluación de las alternativas para gestionar de manera eficiente el espectro utilizado en el marco de las redes de 5G en México.

Sansó-Rubert Pascual, D. (2021). La estrategia de seguridad de la Unión Europea a revisión: una "unión de la seguridad" en clave multidimensional. *La estrategia de seguridad de la Unión Europea a revisión: una "unión de la seguridad" en clave multidimensional*, 63-80.

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.

Zago, M. (2021). Enhancing DGA-based botnet detection beyond 5G with on-Edge machine learning. *Proyecto de investigación*.