Desafíos y vulnerabilidades asociados con la seguridad informática en las redes de generación (NGN) móviles 5G

John Alexander Merchan Castillo

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización de Redes de Nueva Generación

2024

Desafíos y vulnerabilidades asociados con la seguridad informática en las redes de nueva generación (NGN) móviles 5G

John Alexander Merchan Castillo

Asesor

Mónica Andrea Rico Martínez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización de Redes de Nueva Generación

2024

_____

PhD Mauricio Ochoa Sana

_____ _____

Jurado Jurado

2024

Agradecimientos

El autor presenta un cordial saludo y agradecimiento al personal de docentes y administrativos de la Facultad de Ingeniería de Telecomunicaciones de la Universidad NacionalAbierta y a Distancia, quienes, con su gran aporte y colaboración, permitieron el logro de los objetivos propuestos durante el desarrollo de mi carrera profesional.

A la Doctora Mónica Andrea Rico Martínez y al Doctor Mauricio Ochoa Sana por su incondicional asesoría y orientación, durante el desarrollo del proyecto de investigación.

A Dios, por darme la fuerza, la salud y la sabiduría necesarias para llevar a cabo este trabajo. A mi esposa, por su incondicional amor, paciencia y apoyo durante todo este proceso. Tuánimo constante y comprensión han sido fundamentales para la culminación de este proyecto.

A mi madre, por su amor inagotable, sus enseñanzas y su constante motivación para alcanzar mis metas. A mis profesores y mentores, cuyo conocimiento, guía y apoyo han sidoesenciales para el desarrollo y la finalización de esta monografía. Gracias por compartir su experiencia y por sus valiosas sugerencias.

A mis amigos y colegas, por su aliento y compañerismo, que me han ayudado a superar los desafíos a lo largo de esta travesía académica. A todos ustedes, les extiendo mi más profundo agradecimiento. Este logro no habría sido posible sin su apoyo y contribuciones.

Resumen

La transición hacia las redes 5G representa un avance crucial en las telecomunicaciones, permitiendo la implementación de una nueva generación de aplicaciones y servicios críticos. Sin embargo, este progreso trae consigo desafíos significativos en ciberseguridad, debido a la mayor superficie de ataque, la complejidad de la red y la diversidad de aplicaciones soportadas. Esta monografía analiza exhaustivamente las vulnerabilidades inherentes a la arquitectura 5G y propone estrategias de mitigación basadas en la especificación 3GPP TS 33.501. Se evalúan las directrices y prácticas recomendadas por organismos líderes como GSMA, 3GPP, ENISA y NIST, proporcionando un enfoque integral para proteger la infraestructura y los datos en entornos 5G. Entre las estrategias propuestas se incluyen el cifrado de extremo a extremo (E2EE), la autenticación multifactor (MFA) y la segmentación de red (Network Slicing). Estas prácticas son esenciales para asegurar la confidencialidad, integridad y disponibilidad de los datos, permitiendo a las organizaciones operar de manera segura y eficiente. La colaboración entre operadores de redes, proveedores de tecnología y reguladores es fundamental para desarrollar e implementar medidas de seguridad efectivas, garantizando la resiliencia de las redes5G frente a amenazas cibernéticas. Las lecciones aprendidas y las estrategias implementadas en 5G también servirán como base para futuras innovaciones en la seguridad de redes móviles, especialmente con la evolución hacia 6G.

***Palabras clave**:* Ciberseguridad, redes 5G, 3GPP TS 33.501, autenticación multifactor, cifrado de extremo a extremo

Abstract

The transition to 5G networks marks a crucial advancement in telecommunications, enabling the deployment of a new generation of critical applications and services. However, this progress brings significant cybersecurity challenges due to the increased attack surface, network complexity, and diversity of supported applications. This monograph provides a comprehensive analysis of the inherent vulnerabilities in 5G architecture and proposes mitigation strategies based on the 3GPP TS 33.501 specification. It evaluates the guidelines and recommended practices from leading organizations such as GSMA, 3GPP, ENISA, and NIST, offering an integrated approach to protect infrastructure and data in 5G environments. The proposed strategies include end-to-end encryption (E2EE), multifactor authentication (MFA), and networkslicing. These practices are essential to ensure the confidentiality, integrity, and availability of data, allowing organizations to operate securely and efficiently. Collaboration among network operators, technology providers, and regulators is crucial to develop and implement effective security measures, ensuring the resilience of 5G networks against cyber threats. The lessons learned and strategies implemented in 5G will also serve as a foundation for future innovations in mobile network security, especially as the evolution towards 6G progresses.

Keywords: Cybersecurity, 5G networks, 3GPP TS 33.501, multifactor authentication, end-to-end encryption

Tabla de Contenido

Lista de Figuras

Introducción

Las redes 5G representan el futuro de la comunicación inalámbrica, ofreciendo velocidades de transmisión de datos sin precedentes, latencia reducida y una capacidad masiva para conectar dispositivos IoT (Internet de las Cosas). Sin embargo, su implementación trae consigo retos significativos en términos de ciberseguridad, debido a su naturaleza omnipresente y a la cantidad de datos sensibles que gestionará.

La evolución tecnológica hacia la quinta generación de telecomunicaciones, conocida como 5G, marca un hito en la historia de la comunicación inalámbrica. Esta tecnología promete transformar radicalmente nuestras vidas, habilitando velocidades de conexión ultrarrápidas, reduciendo significativamente la latencia y soportando un número exponencialmente mayor de dispositivos conectados simultáneamente. Sin embargo, con estas innovaciones también surgen desafíos sin precedentes en el ámbito de la ciberseguridad, los cuales requieren una atención y soluciones igualmente innovadoras.

La importancia de la ciberseguridad en las redes 5G no puede ser subestimada. A medida que nos adentramos en una era donde la interconexión digital se vuelve cada vez más intrínseca atodos los aspectos de nuestra vida cotidiana y la economía global, la protección de esta infraestructura crítica contra actores maliciosos cobra una relevancia primordial. Las redes 5G, alser el soporte de tecnologías emergentes como las ciudades inteligentes, la cirugía remota, los vehículos autónomos y la Internet de las Cosas (IoT), presentan un conjunto complejo de vulnerabilidades que podrían ser explotadas para comprometer la seguridad de datos sensibles y la integridad de sistemas críticos.

Este trabajo busca explorar en profundidad los desafíos específicos que la ciberseguridadenfrenta en el contexto de las redes 5G, identificando tanto las vulnerabilidades

inherentes a esta nueva tecnología como las estrategias de mitigación propuestas por organismos líderes en el campo, tales como el National Institute of Standards and Technology (NIST) y la Cybersecurity and Infrastructure Security Agency (CISA). A través de un análisis detallado de directrices y estudios de caso, se pretende ofrecer una visión holística que permita a organizaciones y entidades gubernamentales implementar prácticas robustas de ciberseguridad adaptadas a las especificidades de la infraestructura 5G.

En última instancia, el objetivo de esta monografía es no solo arrojar luz sobre la importancia crítica de asegurar las redes 5G frente a amenazas cibernéticas, sino también sugerirun marco de acción que permita a la sociedad aprovechar los beneficios de esta tecnología emergente sin comprometer la seguridad y privacidad de los usuarios. Así, se busca contribuir aldesarrollo de un ecosistema digital más seguro y resiliente, capaz de soportar el avance hacia un futuro cada vez más conectado.

Descripción de la Realidad Problemática

La implementación global de las redes de quinta generación (5G) promete transformar radicalmente el panorama de las telecomunicaciones, ofreciendo velocidades de conexión ultrarrápidas, latencias mínimas y una capacidad sin precedentes para soportar un número masivo de dispositivos conectados simultáneamente. Sin embargo, estas innovaciones no vienensin desafíos, especialmente en el ámbito de la ciberseguridad. La expansión de la superficie de ataque, la introducción de nuevas tecnologías como el Network Slicing y la Computación Multi-acceso en el Borde (MEC), y la complejidad creciente de la gestión de la red plantean vulnerabilidades significativas que deben ser abordadas para proteger la infraestructura crítica y los datos sensibles.

Antecedentes Teóricos

Históricamente, cada nueva generación de redes móviles ha enfrentado sus propios desafíos de seguridad, desde la facilidad de interceptación de llamadas en las redes 2G hasta las vulnerabilidades de seguridad en el intercambio de datos en 4G. Con 5G, la situación se complica aún más debido a su arquitectura inherente y la diversidad de servicios que pretende ofrecer. Investigaciones previas han demostrado la necesidad de un enfoque holístico de seguridad que abarque tanto la protección de la infraestructura como la privacidad de los usuarios. Las lecciones aprendidas de generaciones anteriores enfatizan la importancia de anticipar riesgos y desarrollar soluciones de seguridad robustas desde las fases iniciales de implementación de 5G.

Problema General

¿Cómo pueden las redes 5G ser protegidas efectivamente contra las amenazas de ciberseguridad emergentes y evolutivas, considerando su arquitectura avanzada y la amplia gama de aplicaciones y servicios que soportan?

Problemas Específicos

¿Cuáles son las principales vulnerabilidades asociadas con la arquitectura y las tecnologías subyacentes de las redes 5G, como el Network Slicing y la MEC?

¿Cómo impacta la conectividad masiva del IoT en la superficie de ataque de las redes 5Gy qué medidas pueden implementarse para mitigar estos riesgos?

¿Qué estrategias y prácticas de ciberseguridad pueden desarrollarse para asegurar la comunicación de extremo a extremo en un entorno de red 5G altamente dinámico y distribuido?

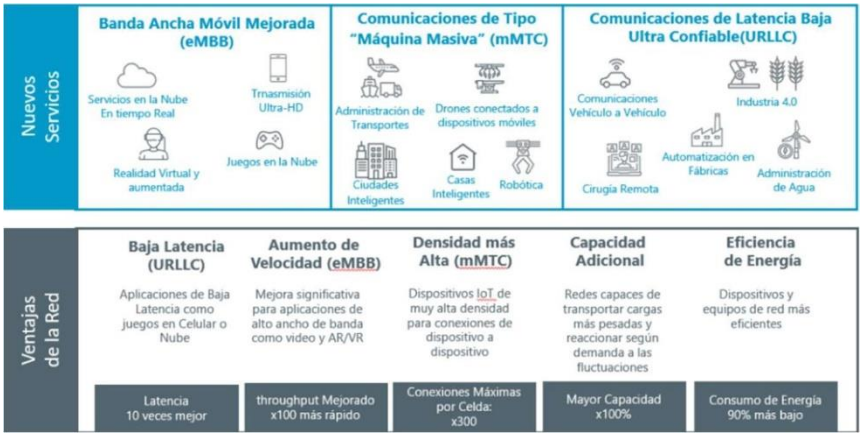
¿De qué manera pueden las lecciones aprendidas de las vulnerabilidades de seguridad en generaciones anteriores de redes móviles aplicarse para fortalecer la seguridad en 5G?

Marco Histórico

La tecnología 5G representa la quinta generación de redes móviles, marcando un avance significativo respecto a sus predecesoras. Introducida comercialmente a partir de 2019, 5G promete transformar radicalmente varios sectores industriales y la vida cotidiana, ofreciendo una conectividad más rápida, fiable y eficiente. A diferencia de las generaciones anteriores, 5G está diseñada para soportar una amplia gama de aplicaciones que requieren gran ancho de banda, bajalatencia y una alta densidad de conexiones, como el Internet de las Cosas (IoT), vehículos autónomos, ciudades inteligentes y aplicaciones de realidad aumentada y virtual.

Figura 1

Nuevos Servicios y Ventajas de la Red 5G



Nota. La imagen ilustra las ventajas y nuevos servicios que ofrece la red 5G, destacando tres categorías principales de servicios y sus beneficios asociados. Adaptado de *Transición de 4G a 5G con RADCOM ACE*, Parte 1 https://radcom.com/transicion-de-4g-a-5g-con-radcom-ace-parte-1/

Nuevos Servicios: Banda Ancha Móvil Mejorada (eMBB), Comunicaciones de Tipo "Máquina Masiva" (mMTC), Comunicaciones de Latencia Baja Ultra Confiable (URLLC),

Ventajas de la Red Baja Latencia (URLLC), Aumento de Velocidad (eMBB), Densidad másAlta (mMTC), Capacidad Adicional, Eficiencia de Energía.

La introducción de 5G conlleva varios cambios fundamentales en la arquitectura de red, incluyendo el uso de frecuencias más altas con bandas de espectro milimétrico, redes densificadas con una mayor cantidad de pequeñas celdas, y tecnologías avanzadas como MIMO masivo y beamforming. Estas innovaciones permiten a 5G alcanzar velocidades de descarga de hasta 20 Gbps y reducir la latencia a menos de 1 milisegundo en condiciones ideales.

Figura 2

¿Que es Mimo?

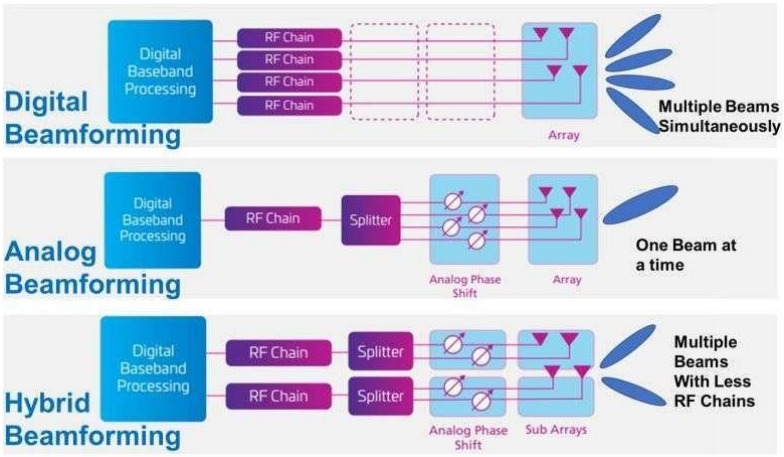
Nota. La imagen ilustra cómo MIMO permite la ampliación de la capacidad mediante la transmisión simultánea de múltiples señales. Una analogía utilizada es la de una avenida saturadaque no se puede ampliar más a lo ancho; sin embargo, se puede construir otra avenida sobre la original, aumentando así su capacidad. Adaptado de *AT: MIMO ADVANCED* febrero 4 2019 AT: MIMO Advanced (arastechnologies.com)

Otra tecnología avanzada utilizada en 5G es el beamforming, que optimiza la dirección de las señales para mejorar la eficiencia y reducir la interferencia. Existen varias formas de

beamforming, incluyendo el digital, analógico e híbrido, cada una con sus propias ventajas y aplicaciones específicas.

Figura 3

Beanforming



Nota. La imagen muestra los diferentes tipos de beamforming utilizados en las redes 5G. El beamforming digital permite múltiples haces simultáneamente, el analógico utiliza un haz a la vez, y el híbrido combina lo mejor de ambos enfoques para manejar múltiples haces con menos cadenas de RF. Adaptado de *thathipsterlife.com*

Sin embargo, la complejidad y las capacidades de 5G también introducen nuevos desafíosde seguridad que deben ser abordados de manera proactiva para proteger la infraestructura de redy los datos transmitidos. Esto incluye la protección contra ataques a la privacidad, la integridad de los datos y la disponibilidad del servicio, lo que requiere un enfoque de seguridad integral queabarque tanto la protección de la red como la de las aplicaciones y servicios que se ejecutan en ella.

El desarrollo de la tecnología 5G representa un avance significativo en la evolución de lastelecomunicaciones móviles. Este salto tecnológico introduce características técnicas

innovadoras diseñadas para satisfacer las crecientes demandas de un mundo digitalmente conectado. A continuación, se destacan los aspectos más relevantes del desarrollo y las características técnicas de las redes 5G.

Velocidades de Transmisión Mejoradas Las redes 5G están diseñadas para ofrecer velocidades de datos mucho más altas que las generaciones anteriores, alcanzando picos teóricos de hasta 20 Gbps. Esto facilita aplicaciones como la transmisión de video de ultra alta definición,juegos en línea con gráficos intensos y el uso de realidad aumentada o virtual sin latencia perceptible. (Saad et al., 2020)

Reducción de Latencia Una de las innovaciones más importantes de 5G es su capacidad para reducir significativamente la latencia, a veces hasta 1 milisegundo. La latencia reducida es crítica para aplicaciones en tiempo real, operaciones de dispositivos autónomos y para habilitar tecnologías emergentes como la conducción de vehículos autónomos y la telemedicina. (Al-Dulaimi et al., 2015).

Conectividad Masiva 5G puede soportar una densidad de conexión considerablemente mayor, con la capacidad de conectar hasta un millón de dispositivos por kilómetro cuadrado. Esto es esencial para el despliegue efectivo del Internet de las Cosas (IoT), donde innumerables dispositivos necesitan estar conectados simultáneamente sin comprometer el rendimiento. (Porambage et al., 2018).

Mayor Eficiencia Energética Además de mejorar la velocidad y la latencia, 5G también introduce mejoras en la eficiencia energética. Esto no solo tiene el potencial de reducir los costosoperativos para los proveedores de servicios sino también de minimizar el impacto ambiental de la red. (Buzzi et al., 2016).

Flexibilidad de la Red A través de tecnologías como la virtualización de funciones de red(NFV) y las redes definidas por software (SDN), 5G ofrece una flexibilidad y escalabilidad sin precedentes. Esto permite a los proveedores de servicios adaptar la red rápidamente para satisfacer las necesidades específicas de diferentes aplicaciones y servicios. (Andrews et al., 2014).

Seguridad Mejorada Aunque la ciberseguridad es un desafío constante, la arquitectura de5G incorpora mejoras significativas en seguridad diseñadas para proteger contra una amplia gama de amenazas cibernéticas.

Los fundamentos teóricos de la seguridad en redes 5G se asientan en la necesidad de proteger la red y sus datos contra accesos no autorizados, manipulación y ataques. Estudios previos han destacado la importancia del cifrado, la autenticación, la integridad de los datos, y laprivacidad como pilares fundamentales. La arquitectura de 5G, con su dependencia de la virtualización y el network slicing, requiere enfoques innovadores de seguridad que sean tanto robustos como flexibles.

Investigaciones o Antecedentes del Estudio

Investigaciones anteriores han identificado vulnerabilidades específicas en las redes 5G, como ataques de denegación de servicio (DoS), interceptaciones y ataques al Internet de las Cosas (IoT). Estudios como los de la GSMA (Global System for Mobile Communications Association) y el 3GPP (3rd Generation Partnership Project) han proporcionado guías y estándares para mitigar estos riesgos. Además, la aplicación de tecnologías emergentes como blockchain y la inteligencia artificial en la seguridad de 5G ha sido objeto de análisis recientes, mostrando un camino prometedor hacia una protección más efectiva. GSMA. (2019). "Mobile Security Research".,3GPP. (2020). "5G Security; Specification of the Security Architecture".

Ataques de Denegación de Servicio (DoS) Estos ataques buscan hacer que los recursos de la red sean inaccesibles para los usuarios legítimos al sobrecargarlos con tráfico malicioso. Enredes 5G, estos ataques pueden ser especialmente perjudiciales debido a la gran cantidad de dispositivos conectados simultáneamente. ENISA. (2019). "Threat Landscape for 5G Networks".

Interceptaciones La interceptación de datos en tránsito es un riesgo significativo en las redes 5G, especialmente debido a la mayor cantidad de puntos de acceso y la utilización de nuevas bandas de espectro. La implementación de cifrado de extremo a extremo es una medida crucial para mitigar este tipo de ataques. ENISA. (2019). "Threat Landscape for 5G Networks".

Ataques al IoT Los dispositivos IoT son particularmente vulnerables debido a sus limitadas capacidades de procesamiento y seguridad. Ataques comunes incluyen la toma de control de dispositivos (botnets), la manipulación de datos y la invasión de la privacidad.

ENISA. (2019). "Threat Landscape for 5G Networks".

Estudios han mostrado cómo tecnologías emergentes pueden ayudar a mejorar la seguridad en redes 5G

Blockchain Blockchain es una plataforma de base de datos descentralizada y peer-to-peer que almacena los bloques de datos de transacciones vinculados entre sí en cadenas. Esta tecnología puede mejorar la seguridad y la integridad de las transacciones y comunicaciones en redes 5G al proporcionar una forma segura e inmutable de registrar datos. IBM. (2020). "Blockchain for Enhanced Network Security".

Inteligencia Artificial (IA) La IA se está utilizando para desarrollar sistemas avanzados de detección y respuesta a amenazas en tiempo real. Algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos para identificar patrones sospechosos y mitigar amenazas antes de que causen daño. NIST. (2020). "Framework for Improving Critical Infrastructure Cybersecurity".

Objetivo General

"Desarrollar estrategias de ciberseguridad basadas en la especificación 3GPP TS 33.501 para mitigar los riesgos en la implementación y uso de redes 5G, garantizando la protección integral de la infraestructura y los datos mediante la implementación de políticas de cifrado avanzadas, autenticación multifactor, segmentación de red y el uso de tecnologías emergentes como la inteligencia artificial y blockchain."

Objetivos Específicos

Identificar las principales vulnerabilidades de ciberseguridad en redes 5G y explorar soluciones para su mitigación.

Evaluar estrategias y directrices de organismos líderes en ciberseguridad para la mitigación de riesgos en redes 5G.(Se puedo identificar en el capitulo 5.5 Estrategias de Mitigación y Protección)

Proponer la implementación de tecnologías y prácticas de seguridad avanzadas en un entorno de proveedor de servicios y administradores de red, como el cifrado de extremo a extremo, autenticación robusta y segmentación de red (Network Slicing) siguiendo los lineamientos de la 3GPP TS 33.501.

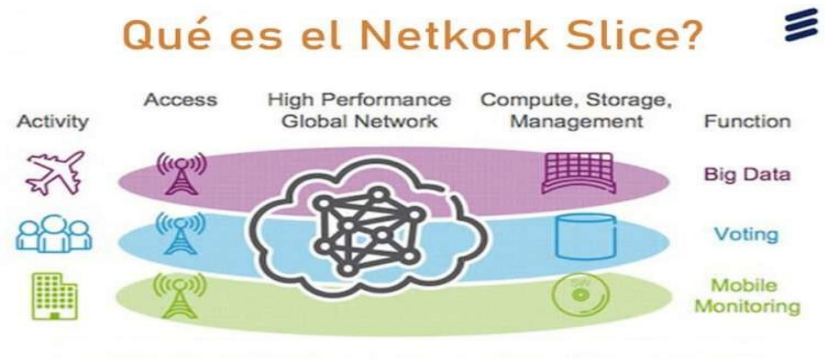
Delimitación de Estudio

Ámbito Geográfico La investigación se centrará en implementaciones y estudios de caso globales, sin limitarse a una región específica, dado el alcance internacional de la tecnología 5G y su impacto a nivel mundial. Sin embargo, se pueden destacar ejemplos particulares de países líderes en la adopción de 5G como Corea del Sur, China, Estados Unidos y naciones de la UniónEuropea.

Aspectos Tecnológicos El estudio se limitará a las vulnerabilidades de seguridad inherentes a la arquitectura de 5G, las tecnologías de red subyacentes (como el slicing de red y la MEC), y los protocolos de seguridad aplicables específicamente en el contexto de 5G. Se excluyen comparaciones directas con generaciones anteriores de tecnologías de red, excepto paradestacar mejoras o nuevas vulnerabilidades introducidas por 5G.

Figura 4

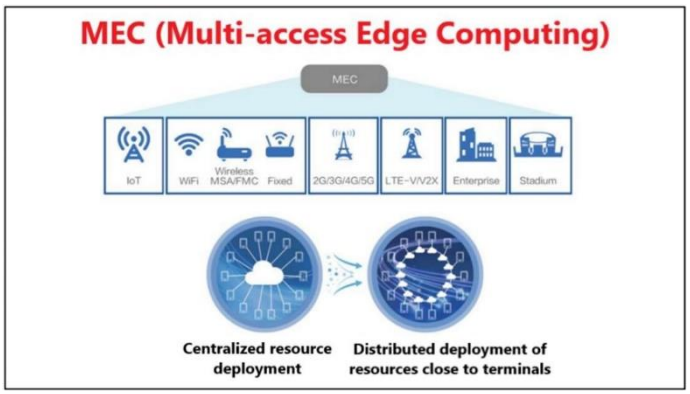
¿Que es Network Slice?



Nota. La imagen muestra cómo el Network Slicing permite la creació de diferentes segmentos de red virtuales, cada uno diseñado para satisfacer requisitos específicos de rendimiento y funcionalidad, tales como Big Data, Voting y Mobile Monitoring. Esta técnica mejora la eficiencia yflexibilidad de la red, permitiendo una gestión más precisa de los recursos de red. Adaptado 30 JUL *¿Qué Es El Network Slicing?*. Fuente: https://centralizate.es/que-es-el-network-slicing/

Figura 5

*MEC (Multi-Access Edge Computing***)**



Nota. La imagen muestra cómo MEC permite el despliegue centralizado de recursos, así como eldespliegue distribuido de recursos cerca de los terminales. Esto mejora significativamente la eficiencia y la capacidad de respuesta de la red, permitiendo una mejor gestión de los servicios y aplicaciones en tiempo real. Adaptado de :[*Introduction to 5G] Multi-Access Edge Computing*, Created: 2021-12-21 02:49:23Latest reply: 2022-03-23 15:59:21[Introduction to 5G] Multi- Access Edge Computing (huawei.com)

Rango Temporal Dado el rápido desarrollo de la tecnología 5G, el estudio se enfocará en literatura, estudios y datos disponibles hasta la fecha actual, con una vista hacia las tendencias emergentes y futuras innovaciones en seguridad hasta el año en curso.

Población y Muestra La investigación se basará en información disponible públicamente,incluyendo estudios académicos, informes técnicos de organizaciones líderes en telecomunicaciones y ciberseguridad (como 3GPP, GSMA, ITU, y NIST), y análisis de seguridad de proveedores de tecnología y operadores de redes. No se realizarán encuestas o estudios primarios específicos.

Enfoque del Estudio Mientras que la ciberseguridad abarca una amplia gama de temas, este estudio se enfocará específicamente en las amenazas a la seguridad informática relacionadas con la infraestructura de red 5G, dejando de lado aspectos como la seguridad física de lasinstalaciones de red.

Justificación e Importancia del Estudio

La relevancia de este estudio se fundamenta en la creciente dependencia de la sociedad enlas tecnologías de comunicación inalámbrica y la necesidad de adherirse a los estándares internacionales de seguridad, específicamente la especificación técnica 3GPP TS 33.501, para proteger las infraestructuras críticas 5G contra amenazas cibernéticas. Como se destaca en la guía de la Cybersecurity and Infrastructure Security Agency (CISA), asegurar la infraestructura 5G es prioritario para proteger las funciones críticas nacionales y la economía digital.

La justificación de esta monografía se fundamenta en la creciente importancia de las redes 5G y los desafíos únicos de ciberseguridad que presentan. A medida que el mundo se mueve hacia una adopción más amplia de esta tecnología, se hace evidente la necesidad de abordar proactivamente las vulnerabilidades de seguridad para proteger los datos y sistemas críticos. Este estudio es pertinente y necesario por varias razones clave

Impacto Transformador de 5G Las redes 5G prometen revolucionar industrias enteras, mejorando la conectividad, la eficiencia y la capacidad de innovación en campos como el transporte, la salud y la manufactura. Sin embargo, el potencial completo de 5G solo puede ser alcanzado si las infraestructuras subyacentes son seguras y confiables.

Aumento de la Superficie de Ataque La arquitectura de 5G, con su mayor uso de software y la densidad de dispositivos conectados, expande significativamente la superficie de ataque, presentando nuevas oportunidades para actores maliciosos. Abordar estas

vulnerabilidades a través de estrategias de ciberseguridad sólidas es crucial para prevenir ataquesque podrían tener consecuencias devastadoras en la economía y la seguridad nacional.

Necesidad de Estrategias de Seguridad Actualizadas Las prácticas de ciberseguridad existentes, diseñadas para redes anteriores, pueden no ser efectivas contra las amenazas dirigidasa las redes 5G. La investigación y el desarrollo de enfoques novedosos son esenciales para mantenerse adelante de las tácticas en evolución de los ciberdelincuentes.

Relevancia para la Toma de Decisiones Políticas y Empresariales Al proporcionar un análisis detallado de los riesgos de ciberseguridad en 5G y las estrategias de mitigación, esta monografía sirve como una herramienta valiosa para formuladores de políticas, reguladores y líderes empresariales que buscan tomar decisiones informadas sobre el despliegue y la gestión deinfraestructuras 5G.

Contribución al Conocimiento Académico Este trabajo también busca llenar un vacío en la literatura académica existente sobre ciberseguridad en 5G, ofreciendo análisis, perspectivas y recomendaciones basadas en las últimas investigaciones y mejores prácticas en el campo.

Supuestos Teóricos

Se asume que la arquitectura y tecnologías subyacentes a las redes 5G introducen vulnerabilidades únicas que requieren estrategias de mitigación específicas. Además, se presupone que la eficacia de estas estrategias puede medirse a través de indicadores específicos de seguridad.

Hipótesis General

La implementación de estrategias de seguridad robustas y específicamente diseñadas para5G puede mitigar significativamente las vulnerabilidades asociadas con su arquitectura y tecnologías subyacentes, mejorando la resiliencia de la red frente a ciberataques.

Hipótesis Específicas

La segmentación de red y el network slicing en 5G, cuando se implementan con políticas de seguridad adecuadas, reducen la superficie de ataque y limitan el impacto de posibles brechas de seguridad. El uso de tecnologías avanzadas de cifrado y autenticación robusta en las comunicaciones 5G protege contra interceptaciones y accesos no autorizados. La adopción de soluciones de inteligencia artificial para el monitoreo y la respuesta a amenazas en tiempo real mejora la capacidad de detección y prevención de ataques en redes 5G.

Variables Principales

Vulnerabilidad de la Red Grado en que la infraestructura 5G es susceptible a ciberataques.

Estrategias de Mitigación Conjunto de políticas, tecnologías y prácticas implementadas para proteger la red 5G.

Definiciones Operacionales

Vulnerabilidad de la Red Medida por el número de incidentes de seguridad reportados enun período específico y la gravedad de estos. Estrategias de Mitigación Evaluar la implementación de políticas de seguridad,tecnologías de cifrado, autenticación y monitoreo en la infraestructura 5G.

Indicadores

Para Vulnerabilidad de la Red: Número de ataques exitosos, tipos de ataques más comunes, tiempo promedio para detectar y contener ataques.Para Estrategias de Mitigación Nivel de implementación de cifrado de extremo a extremo, porcentaje de tráfico monitoreado por soluciones de IA, tiempo promedio de respuestaa incidentes de seguridad.

Técnica e InstrumentoTipo de la Investigación

La investigación se clasifica como descriptiva y analítica. Se enfocará en describir y analizar las vulnerabilidades de seguridad en redes 5G y las estrategias para su mitigación, utilizando un enfoque cualitativo para profundizar en el entendimiento de estos aspectos críticos.

Diseño para Utilizar. El estudio utilizará un diseño no experimental, transversal. Este diseño es adecuado para investigaciones que buscan observar y describir características de un fenómeno en un momento específico sin manipular variables.

Universo Todas las redes 5G desplegadas globalmente.

Población Infraestructuras de red 5G que han sido objeto de estudios de seguridad y análisis de vulnerabilidad.

Muestra Un conjunto representativo de estudios de caso sobre seguridad en redes 5G, seleccionados basándose en su relevancia, profundidad de análisis y diversidad geográfica.

Muestreo Se realizará un muestreo no probabilístico por conveniencia, eligiendoestudios y reportes accesibles públicamente que provean insights significativos sobre la seguridad en redes 5G.

Técnicas Revisión bibliográfica de fuentes secundarias, incluyendo artículosacadémicos, informes técnicos de organizaciones líderes en telecomunicaciones y ciberseguridad, y análisis de casos de estudio.

Instrumentos Se utilizará una matriz de análisis documental para organizar y sintetizar la información recolectada de las fuentes secundarias.

Procesamiento de Datos El procesamiento de datos se realizará a través del análisis cualitativo de contenido. Se identificarán patrones, temas y categorías relacionados con las

vulnerabilidades de seguridad en 5G y las estrategias de mitigación. Se emplearán herramientas de software de análisis cualitativo,como NVivo o ATLAS.ti, para facilitar la codificación, el análisis y la visualización de datos.

La administración del proyecto de investigación sobre la ciberseguridad en redes 5G implicará la coordinación de actividades de investigación, revisión de literatura, análisis de datos, y redacción del informe final. Se asignarán responsabilidades específicas para asegurar una gestión eficiente del tiempo y los recursos disponibles.

Marco Conceptual

La evolución de la ciberseguridad en las redes móviles ha sido un viaje continuo de adaptación y mejora, avanzando a la par con las generaciones sucesivas de tecnologías de telecomunicaciones. Desde los inicios de la telefonía móvil hasta la era del 5G, cada generación ha presentado nuevos desafíos y soluciones en ciberseguridad.

1G y 2G En las primeras etapas de la telefonía móvil, particularmente con 1G y 2G, la ciberseguridad no era una preocupación principal. La primera generación (1G) se basaba en tecnología analógica y estaba principalmente enfocada en la voz. Con la introducción de 2G, comenzó el uso de tecnología digital, lo que aumentó las capacidades de la red pero también introdujo los primeros desafíos significativos de seguridad, como la clonación de teléfonos y el fraude (Jover, 2009).

3G La tercera generación (3G) trajo mejoras considerables en seguridad, introduciendo características como el cifrado de datos y la autenticación más robusta entre el dispositivo y la red. Estas medidas buscaban abordar las vulnerabilidades de privacidad y seguridad evidenciadasen las generaciones anteriores (Kambourakis et al., 2005).

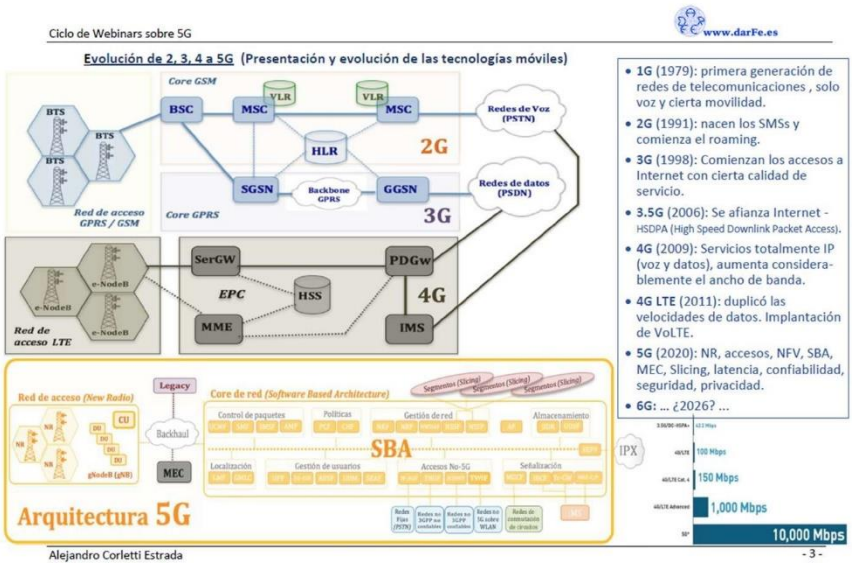
4G/LTE Con 4G/LTE, la industria enfrentó el desafío de asegurar una infraestructura completamente IP, lo que planteó riesgos significativos en términos de ataques de denegación deservicio (DoS), interceptación de datos y otros tipos de ciberataques más sofisticados. Esto llevó al desarrollo de estándares y prácticas de seguridad más avanzados, centrándose en la protecciónde la integridad y la confidencialidad de los datos (Forsberg et al., 2007).

Hacia el 5G La transición hacia el 5G ha requerido un replanteamiento aún más profundo de la ciberseguridad, dada la complejidad de su arquitectura, la diversidad de servicios

que soporta y su integración con el Internet de las Cosas (IoT). Se han introducido conceptos como la "seguridad por diseño" y la segmentación de la red para proporcionar una protección integral y adaptativa a lo largo de la red 5G (Ala et al., 2020).

Figura 6

Evolución de las Tecnología Móviles



Nota. 5G La quinta generación de tecnología de redes móviles, diseñada para aumentar la velocidad, reducir la latencia y permitir una mayor conectividad de dispositivos. Adaptado de *Corletti Estrada, A. (2020). Ciclo de Webinars sobre 5G Presentación e introducción a 5G.* Recuperado de https://www.youtube.com/watch?v=0m9e0mpp2zo&list=PL0QSAEWH0x_hXbHJGO7EPg2iy0gQmU1Tn

Ciberseguridad Medidas de protección aplicadas a redes y dispositivos para prevenir, detectar y responder a ataques cibernéticos.

Network Slicing La capacidad de crear múltiples redes virtuales independientes sobre una misma infraestructura física en redes 5G.

Computación Multi-acceso en el Borde (MEC) Una red arquitectónica que permite el procesamiento de datos y recursos computacionales en el borde de la red, cerca del usuario final.

IoT (Internet de las Cosas) La interconexión de dispositivos cotidianos a través de Internet, permitiendo el intercambio y la recolección de datos.

Vulnerabilidad Una debilidad en un sistema que puede ser explotada por una amenaza para realizar acciones no autorizadas.

Autenticación Proceso de verificación de la identidad de un usuario o dispositivo, asegurando que quien accede a la red es quien dice ser.

Desafíos de Ciberseguridad en Redes 5GVulnerabilidades

Las redes 5G, al igual que cualquier tecnología avanzada, presentan vulnerabilidades específicas que podrían ser explotadas por actores maliciosos. Estas vulnerabilidades se derivan de la complejidad de la infraestructura 5G, su dependencia de software y la amplia gama de servicios y aplicaciones que soporta. A continuación, se detallan algunas de las posibles vulnerabilidades específicas de las redes 5G.

Superficie de Ataque Expandida La densidad de dispositivos conectados y la infraestructura virtualizada amplían las oportunidades para los atacantes. La implementación del Internet de las Cosas (IoT) y el aumento masivo en el número de dispositivos conectados a travésde redes 5G amplían significativamente la superficie de ataque. Esto puede incrementar las oportunidades para que los ciberdelincuentes lancen ataques distribuidos de denegación de servicio (DDoS) y otros tipos de ataques basados en la red (Chowdhury et al., 2020).

Interfaz Aérea Expuesta El aumento de los puntos de acceso inalámbrico y el uso de nuevas bandas de espectro pueden ofrecer nuevos vectores de ataque.

Riesgos de Seguridad de la Cadena de Suministro La dependencia de hardware y software de múltiples proveedores introduce riesgos de vulnerabilidades incorporadas o puertas traseras.

Configuración y Gestión Complejas La complejidad de las configuraciones de red y la gestión de políticas pueden llevar a errores que comprometan la seguridad.

Ataques a la Capa de Red Dada la naturaleza más abierta y software-dependiente de la arquitectura 5G, existe un riesgo elevado de ataques a la capa de red, incluyendo la intercepción de datos, manipulación de tráfico y ataques de "man-in-the-middle". Estos ataques podrían comprometer la confidencialidad e integridad de los datos transmitidos (Petit et al., 2015).

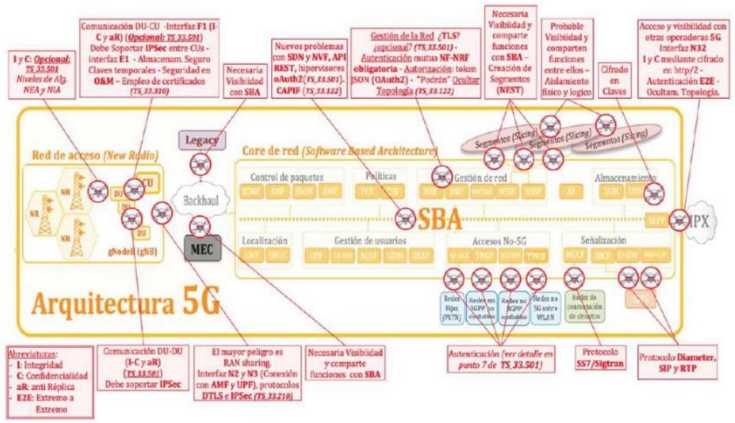
Vulnerabilidades en la Cadena de Suministro La compleja cadena de suministro de componentes y software que conforman las redes 5G introduce riesgos de seguridad, donde un componente comprometido podría ser utilizado como vector de ataque para comprometer toda lared (ENISA, 2019).

Vulnerabilidades de Software y Configuración Las redes 5G dependen en gran medida del software para su operación, lo que las hace susceptibles a vulnerabilidades de software y configuración incorrecta. Estos problemas podrían ser explotados para obtener acceso no autorizado a la red o para desplegar malware (Akhoundi et al., 2013).

Seguridad de la Slicing de Red La tecnología de slicing de red en 5G permite la creación de múltiples redes virtuales sobre una infraestructura física común. Cada slice podría tener diferentes requisitos de seguridad, y una mala configuración o gestión podría exponer datos sensibles o servicios críticos a ataques (Khan et al., 2019).

Figura 7

Arquitectura en Seguridad de Redes 5G



Nota. La imagen muestra la arquitectura de seguridad en redes 5G, resaltando los diferentes puntos de vulnerabilidad y las soluciones propuestas para mitigar estos riesgos. Incluye aspectos como la comunicación DU-CU, la gestión de red, la autenticación mutua NF-NRF, y la segmentación de red.Tipos de ataques cibernéticos que pueden afectar a las redes 5G. Ataques que afectan 5G Adapatado de. *Corletti Estrada, A. (2020). Ciclo de Webinars sobre 5G Presentación e introducción a 5G.* https://www.youtube.com/watch?v=0m9e0mpp2zo&list=PL0QSAEWH0x_hXbHJGO7EPg2iy0gQmU1Tn&index=1

Componentes Clave y Áreas de Seguridad

Red de Acceso (New Radio - NR)

DU y CU (Distributed Unit y Central Unit) Estos componentes son fundamentales en la red de acceso de 5G, encargados de procesar el tráfico de radiofrecuencia y la gestión de la comunicación entre los dispositivos y la red central.

MEC (Multi-access Edge Computing) Permite procesar datos más cerca de donde se generan, reduciendo la latencia y mejorando la eficiencia. Es crucial proteger los datos y las aplicaciones que se ejecutan en el borde de la red.

Seguridad entre DU-CU y MEC La comunicación entre estos componentes debe ser segura, utilizando protocolos como IPSec para asegurar la integridad y confidencialidad de los datos.

Core de la Red (SBA - Software-Based Architecture)

Segmentación de la Red (Slicing) Permite crear múltiples redes virtuales sobre una infraestructura física común. Cada slice debe estar aislado y tener sus propias políticas de seguridad para evitar la propagación de ataques entre slices.

Gestión de Red Incluye la administración de políticas, gestión de usuarios y control de tráfico. Es esencial asegurar la autenticación y autorización de los usuarios y dispositivos.

Control de Paquetes y Políticas La red debe implementar mecanismos de control de tráfico y políticas de seguridad que aseguren la integridad y disponibilidad del servicio.

Almacenamiento y Señalización Los datos almacenados y la señalización entre componentes deben estar protegidos para evitar accesos no autorizados y manipulaciones.

Desafíos de Seguridad y Soluciones

Comunicación DU-CU y MEC

IPSec y Claves Temporales La comunicación entre DU-CU y MEC debe ser segura utilizando IPSec. Las claves temporales y la seguridad en Operación y Mantenimiento (O&M) son cruciales para proteger los datos en tránsito.

Gestión de la Red y Autenticación

Autenticación Mutua NF-NRF La autenticación mutua es obligatoria para asegurar que solo las entidades autorizadas puedan acceder a los recursos de la red. La autorización mediante OAuth2 y la ocultación de topología son medidas adicionales para proteger la red.

Segmentación y Aislamiento

Aislamiento Físico y Lógico La segmentación de la red debe asegurar que cada slice estéaislado física y lógicamente para evitar que un ataque en un slice afecte a otros.

Visibilidad y Compartición de Funciones SBA y Visibilidad Compartida Es necesario que las funciones dentro de la arquitecturaSBA compartan visibilidad y datos de seguridad para detectar y mitigar amenazas de manera efectiva.

Protección de Datos y Cifrado

Cifrado de Extremo a Extremo (E2E) La comunicación y los datos deben estar cifrados desde el origen hasta el destino para proteger la confidencialidad e integridad de los datos.

Las redes 5G, como cualquier tecnología avanzada, están sujetas a una variedad de ataques cibernéticos. La evolución hacia 5G no solo trae consigo mejoras en velocidad y capacidad sino también nuevos desafíos de seguridad que requieren atención. A continuación, seenumeran y describen algunos tipos de ataques cibernéticos específicos que pueden afectar a las redes 5G.

Ataques de Denegación de Servicio (DoS) y Ataques Distribuidos de Denegación de Servicio (DDoS) Estos ataques buscan sobrecargar la red y sus recursos, haciendo que los servicios sean inaccesibles para los usuarios legítimos. La densidad de dispositivos y la conectividad omnipresente en 5G aumentan el potencial impacto de estos ataques (Chowdhury etal., 2020).

Ataques Man-in-the-Middle (MitM) En este tipo de ataque, el atacante intercepta la comunicación entre dos partes sin que ellas lo sepan, pudiendo robar, modificar o espiar la información transmitida. Las redes 5G, al ser altamente dependientes de la tecnología inalámbrica y software, pueden ser vulnerables a este tipo de ataques si no se implementan adecuadas medidas de seguridad (Petit et al., 2015).

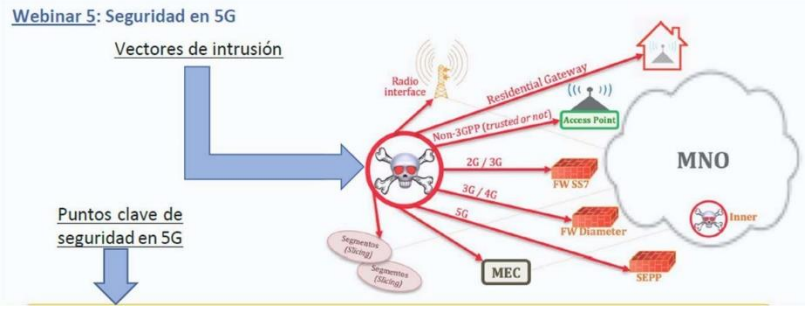
Spoofing e Impersonación Los atacantes pueden falsear la identidad de un dispositivo o usuario para ganar acceso no autorizado a la red o a recursos específicos. Esto puede incluir la suplantación de estaciones base 5G para distribuir comandos maliciosos a dispositivos conectados (ENISA, 2019).

Ataques de Inyección A través de vulnerabilidades en la red o aplicaciones, los atacantes pueden inyectar código malicioso para manipular servicios o robar datos. Las complejas infraestructuras de las redes 5G pueden ofrecer múltiples puntos de entrada para este tipo de ataques (Akhoundi et al., 2013).

Explotación de Vulnerabilidades en la Cadena de Suministro La seguridad de una red 5G puedeverse comprometida por componentes o software malicioso introducido en cualquier punto de la cadena de suministro. Esto requiere un control riguroso y verificación de todos los elementos involucrados en la red (ENISA, 2019).

Figura 8

Vectores de Intrusión en Redes 5G



Nota. Los principales vectores de intrusión en redes 5G y destaca los puntos clave de seguridad que deben ser protegidos para asegurar la integridad y confidencialidad de la red. Se presentan las diferentes interfaces y componentes de la red que pueden ser vulnerables a ataques y las medidas de seguridad necesarias para mitigarlosFuente: Corletti Estrada, A. (2020). Ciclo de Webinars sobre 5G Presentación e introducción a 5G. Adapatado de https://www.youtube.com/watch?v=0m9e0mpp2zo&list=PL0QSAEWH0x_hXbHJGO7EPg2iy0gQmU1Tn&index=1

La imagen ilustra los principales vectores de intrusión en redes 5G y destaca los puntos clave de seguridad que deben ser protegidos para asegurar la integridad y confidencialidad de la red. Se presentan las diferentes interfaces y componentes de la redque pueden ser vulnerables a ataques y las medidas de seguridad necesarias para mitigarlos.

Componentes Clave y Vectores de Intrusión

Interfaces de Radio

Vulnerabilidad Las interfaces de radio son susceptibles a diversos tipos de ataques debido a la naturaleza inalámbrica de la comunicación.

Medida de Seguridad Implementar cifrado robusto y autenticación en lascomunicaciones de radio para proteger contra intercepciones y manipulaciones.

Residential Gateway y Access Points

Vulnerabilidad Los puntos de acceso y gateways residenciales pueden ser objetivos de ataques si no están adecuadamente asegurados.

Medida de Seguridad Asegurar estos dispositivos mediante configuraciones seguras, autenticación robusta y actualizaciones de firmware.

Non-3GPP Interfaces

Vulnerabilidad Interfaces no estandarizadas por 3GPP pueden ser puntos de entrada para atacantes si no se implementan correctamente.

Medida de Seguridad Asegurar la interoperabilidad y compatibilidad de seguridad con las interfaces 3GPP, utilizando protocolos de seguridad adecuados.

Segmentos de Red (Slicing)

Vulnerabilidad La segmentación de la red en slices virtuales puede ser explotada si no se mantiene un aislamiento adecuado entre ellos.

Medida de Seguridad Aislar cada slice con políticas de seguridad específicas y monitorear continuamente para detectar accesos no autorizados.

MEC (Multi-access Edge Computing)

Vulnerabilidad MEC introduce riesgos adicionales debido a la descentralización del procesamiento de datos, aumentando la superficie de ataque.

Medida de Seguridad Implementar cifrado de extremo a extremo y asegurar las comunicaciones entre MEC y otros componentes de la red.

Componentes Internos del MNO (Mobile Network Operator)FW SS7 y FW Diameter

Vulnerabilidad Los firewalls SS7 y Diameter son cruciales para proteger las señales dela red móvil contra ataques de señalización.

Medida de Seguridad Configurar y mantener estos firewalls correctamente para asegurar la integridad de la señalización.

SEPP (Security Edge Protection Proxy)

Vulnerabilidad SEPP protege las comunicaciones entre diferentes operadores de red móvil, siendo un punto crítico de seguridad.

Medida de Seguridad Implementar autenticación mutua y cifrado robusto para proteger estas comunicaciones.

Segmentación de Red y Slicing Seguro Implementar técnicas de segmentación de red y slicing de red para aislar recursos críticos y limitar el impacto de posibles brechas de seguridad.

Cifrado de Extremo a Extremo Utilizar cifrado de extremo a extremo para proteger la transmisión de datos contra interceptaciones y manipulaciones no autorizadas.

Gestión de Identidades y Accesos (IAM) Aplicar políticas de IAM robustas, incluida la autenticación multifactor (MFA), para asegurar el acceso a la red y sus recursos.

Actualizaciones y Parches de Seguridad Mantener los sistemas actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas.

Monitoreo y Detección de Amenazas Implementar soluciones de seguridad avanzadas que permitan la detección en tiempo real de actividades sospechosas o maliciosas.

Evaluaciones de Seguridad y Pruebas de Penetración Realizar evaluaciones periódicas deseguridad y pruebas de penetración para identificar y abordar proactivamente las vulnerabilidades.

Arquitectura de Seguridad 5G Descripción de los componentes de seguridad en 5G según la especificación, incluyendo elementos como el SEPP (Security Edge Protection Proxy) ylas técnicas de protección de la interfaz aérea.

Procedimientos de Seguridad Detalle de los procedimientos de autenticación y autorización, protección de la integridad de los datos y mecanismos de confidencialidad.

Evaluación de Conformidad Análisis de cómo las redes actuales se alinean con las recomendaciones de la 3GPP TS 33.501 y qué mejoras son necesarias para cumplir con estos estándares.

Principios de Ciberseguridad Aplicados a 5G Confidencialidad, Integridad y Disponibilidad (CIA)

La arquitectura de las redes 5G introduce un paradigma avanzado diseñado para soportar una amplia variedad de servicios y aplicaciones, desde comunicaciones móviles de alta velocidadhasta el Internet de las Cosas (IoT), pasando por aplicaciones críticas que requieren baja latencia y alta fiabilidad. Esta nueva generación de redes se basa en una arquitectura flexible y escalable, que incluye tecnologías clave como la virtualización de funciones de red (NFV), las redes definidas por software (SDN), el slicing de red y la computación en el borde (MEC). Sin embargo, estos avances también presentan nuevos desafíos de seguridad que deben ser abordados para asegurar la protección integral de la infraestructura y los datos.

Desafíos de Seguridad en la Arquitectura 5G

Superficie de Ataque Ampliada La densificación de la red y el uso de un mayor número de dispositivos IoT expanden la superficie de ataque, aumentando los puntos vulnerables a ciberataques.

Virtualización y Slicing de Red Aunque la NFV y el slicing de red aportan flexibilidad y eficiencia, también introducen complejidad en la gestión de la seguridad. La segmentación de la red en múltiples "slices" virtuales requiere garantizar la seguridad y el aislamiento entre estos segmentos para evitar que un ataque en uno afecte a los demás.

Seguridad de la Interfaz Aérea Con el aumento de las tasas de transmisión de datos y el uso de nuevas bandas de frecuencia, proteger la transmisión de datos entre los dispositivos y las estaciones base se vuelve más crítico y desafiante.

Dependencia del Software La mayor dependencia del software en la infraestructura de red 5G plantea riesgos de seguridad asociados con vulnerabilidades de software, requiriendo

actualizaciones regulares y gestión de parches para mitigar las amenazas. Interconexión e Interoperabilidad La necesidad de asegurar la interoperabilidad y la interconexión segura entre redes 5G y otras redes (como 4G y redes fijas) presenta desafíos encuanto a compatibilidad de seguridad y gestión de políticas de seguridad unificadas.

Computación Multi-acceso en el Borde (MEC) y Network SlicingComputación Multi-acceso en el Borde (MEC)

Definición MEC es una arquitectura de red que permite procesar datos al borde de la red,más cerca de donde se generan, en lugar de enviarlos a centros de datos centralizados. Esto reduce la latencia, mejora las velocidades de procesamiento y reduce la congestión en la red.

Desafíos de Seguridad en MEC

Seguridad de Datos Al procesar datos sensibles localmente, se debe garantizar que estos están protegidos contra accesos no autorizados.

Gestión de Identidad y Acceso

Es crucial asegurar que solo los dispositivos y usuariosautorizados puedan acceder a las aplicaciones y servicios proporcionados a través de MEC.

Consistencia en la Política de Seguridad Mantener políticas de seguridad consistentes a través de múltiples puntos de procesamiento en el borde puede ser complejo.

Network Slicing, definición permite dividir una sola infraestructura de red física en múltiples redes virtuales, cada una de las cuales puede ser personalizada para satisfacer las necesidades específicas de diferentes aplicaciones o servicios.

Desafíos de Seguridad en Network Slicing

Aislamiento de Slices, es vital asegurar que los slices de red estén completamente aislados entre sí para prevenir el cruce de datos y posibles ataques entre slices.

Gestión de la Seguridad, a Escala a medida que el número de slices de red aumenta, gestionar de manera efectiva la seguridad y mantener la visibilidad completa sobre cada slice se vuelve desafiante.

Consistencia en la Aplicación de Seguridad

Asegurar que las políticas y medidas de seguridad se apliquen de manera consistente en todos los slices es crucial para proteger contravulnerabilidades.

Principios de Ciberseguridad

Confidencialidad, Integridad y Disponibilidad (CIA)

Los principios de Confidencialidad, Integridad y Disponibilidad, conocidos colectivamente como el triángulo CIA, son fundamentales en el campo de la ciberseguridad y son igualmente aplicables en la infraestructura y servicios de 5G. Estos principios guían el desarrollo de políticas y tecnologías de seguridad para proteger la información y los sistemas de información contra el acceso no autorizado, el uso indebido, la divulgación, la interrupción, la modificación o la destrucción.

Confidencialidad en 5G

Se refiere a la protección de la información para que solo aquellos con los derechos y privilegios adecuados puedan acceder a ella. En el contexto de 5G,esto implica el uso de técnicas avanzadas de cifrado y mecanismos de autenticación para proteger los datos transmitidos a través de la red y almacenados en dispositivos conectados a ella. La confidencialidad es crucial para proteger la información sensible del usuario y la propiedad intelectual de las empresas (Ala et al., 2020).

Integridad en 5G

Asegura que la información y los sistemas estén protegidos contra modificaciones o manipulaciones no autorizadas. La integridad de los datos en las redes 5G se mantiene mediante la implementación de controles como firmas digitales y funciones hashcriptográficas, que verifican que los datos no hayan sido alterados desde su origen hasta sudestino. Esto es vital para garantizar la precisión y confiabilidad de la comunicación en aplicaciones críticas como telesalud y sistemas de transporte inteligente (Porambage et al., 2018).

Disponibilidad en 5G

Este principio implica asegurar que la información y los servicios estén disponibles para los usuarios autorizados cuando los necesiten. En el entorno de 5G, la disponibilidad puede verse comprometida por ataques de Denegación de Servicio (DoS) o fallosen la infraestructura de red. Para contrarrestar esto, las redes 5G adoptan una arquitectura resiliente y técnicas como la distribución de carga y redundancia de sistemas para minimizar el impacto de los ataques y garantizar la continuidad del servicio (Chowdhury et al., 2020).

Principios de Diseño Seguro

La adopción de principios de diseño seguro en las redes 5G es fundamental para mitigar los riesgos y amenazas inherentes a esta avanzada tecnología. Estos principios guían el desarrollode la infraestructura y servicios de 5G para asegurar que la seguridad esté integrada en todas las fases del diseño y operación.

Seguridad por Diseño

Este principio implica la integración de medidas de seguridad desde las primeras etapas del diseño de la red. Esto incluye la evaluación de riesgos, la selecciónde arquitecturas seguras y el uso de componentes y protocolos que han sido diseñados teniendo en cuenta la seguridad.

La seguridad por diseño asegura que las medidas de protección sean inherentes al sistema, en lugar de ser añadidas posteriormente (ENISA, 2019).

Minimización de Datos en las redes 5G deben implementar estrategias de minimización dedatos para recopilar, procesar y almacenar solo la información necesaria para el propósito previsto. Esto reduce la exposición a ataques de datos y ayuda a proteger la privacidad del usuario (GSMA, 2020).

Cifrado Integral El uso extensivo de cifrado para proteger los datos en tránsito y en reposo es crucial en redes 5G. Esto incluye el cifrado de comunicaciones entre dispositivos y estaciones base, así como el cifrado de datos almacenados en la red. El cifrado ayuda a asegurar la confidencialidad y la integridad de la información (3GPP, 2020).

Autenticación y Autorización Robustas Implementar sistemas de autenticación y autorización fuertes es esencial para verificar la identidad de los usuarios y dispositivos, y controlar el acceso a recursos de red. Esto incluye el uso de autenticación multifactor y la gestiónde identidades y accesos (IAM) (NIST, 2020).

Segmentación de Red y Slicing La segmentación de red y el slicing permiten dividir la red en segmentos o slices virtuales, cada uno con su propia configuración de seguridad. Esto facilita la implementación de políticas de seguridad diferenciadas, basadas en el nivel de riesgo ylos requisitos específicos de cada slice o segmento (ITU, 2020).

Estrategias de Mitigación y Protección

En el contexto de la ciberseguridad, especialmente relevante para las redes 5G, es crucialdiferenciar entre estrategias proactivas de prevención y estrategias reactivas de respuesta.

Estrategias Proactivas de Prevención

Evaluaciones de riesgo y análisis de vulnerabilidades, realizar evaluaciones regulares de riesgos y análisis de vulnerabilidades para identificar y mitigar posibles brechas de seguridad antes de que sean explotadas (ENISA, 2020).

Educación y capacitación en concienciación de seguridad, proporcionar formación continua a los empleados y usuarios sobre las mejores prácticas de seguridad y concienciación sobre las amenazas cibernéticas actuales (NIST, 2020).

Cifrado y seguridad de datos Utilizar cifrado para proteger los datos en tránsito y en reposo, asegurando que la información sensible esté cifrada y sea inaccesible para los actores maliciosos (GSMA, 2019).

Políticas de Cifrado Avanzadas

Cifrado de Extremo a Extremo (E2EE), la especificación 3GPP TS 33.501 enfatiza la importancia del cifrado de extremo a extremo para proteger los datos tanto en tránsito como en reposo. El uso de E2EE garantiza que la información se cifra en el punto de origen y solo se descifra en el punto de destino, evitando que actores maliciosos intercepten y accedan a los datosdurante su transmisión.

Cifrado de Interfaz Aérea, la protección de la interfaz aérea es crítica en redes 5G debido al aumento de los puntos de acceso inalámbrico y al uso de nuevas bandas de espectro. La especificación recomienda el uso de algoritmos de cifrado robustos como el 256-bit Advanced Encryption Standard (AES) para asegurar la confidencialidad e integridad de los datos transmitidos entre los dispositivos y las estaciones base.

Autenticación Multifactor (MFA), la especificación 3GPP TS 33.501 resalta la implementación de autenticación multifactor como una medida esencial para verificar la

identidad de usuarios y dispositivos antes de permitir el acceso a la red. MFA puede incluir una combinación de factores como contraseñas, biometría (huellas digitales, reconocimiento facial) y tokens de hardware, proporcionando una capa adicional de seguridad y reduciendo significativamente el riesgo de accesos no autorizados.

Autenticación Basada en Certificados El uso de certificados digitales para la autenticación de dispositivos y servicios en la red 5G asegura que solo los dispositivos autorizados puedan acceder y comunicarse dentro de la red. La gestión de certificados debe seguir las mejores prácticas de la Public Key Infrastructure (PKI), incluyendo la emisión, renovación y revocación de certificados.

Técnicas de Aislamiento y Segmentación de la Red

Network Slicing Una de las características distintivas de las redes 5G es la capacidad de crear múltiples redes virtuales independientes sobre una infraestructura física compartida, conocida como Network Slicing. La especificación 3GPP TS 33.501 recomienda la implementación de técnicas de aislamiento robustas entre estos slices para evitar la propagación de ataques y asegurar que una brecha en un slice no afecte a los demás. Cada slice puede tener políticas de seguridad específicas adaptadas a sus requisitos y nivel de riesgo.

Segmentación de Red La segmentación de la red implica dividir la red en segmentos máspequeños y gestionar cada uno con políticas de seguridad específicas. Esta técnica limita la capacidad de los atacantes para moverse lateralmente dentro de la red y reduce la superficie de ataque. La especificación sugiere el uso de tecnologías como Virtual LANs (VLANs) y Virtual Private Networks (VPNs) para implementar la segmentación efectiva.

Monitoreo y Detección de Amenazas

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) La especificación 3GPP TS 33.501 recomienda la implementación de sistemas IDS/IPS avanzados para monitorear el tráfico de red en tiempo real y detectar actividades sospechosas o maliciosas. Estos sistemas pueden bloquear automáticamente las amenazas antes de que causen daño, protegiendo la infraestructura de red y los datos sensibles.

Monitoreo Continuo y Análisis de Seguridad El monitoreo continuo de la red, combinado con el análisis avanzado de seguridad, es crucial para identificar y responder rápidamente a las amenazas emergentes. Herramientas como Security Information and Event Management (SIEM) pueden consolidar datos de múltiples fuentes, proporcionar visibilidad integral de la red y permitir la respuesta proactiva a incidentes de seguridad.

Actualizaciones y Gestión de Parches

Actualización Regular de Software y Parches de Seguridad Mantener el software y el firmware actualizados es fundamental para proteger la red contra vulnerabilidades conocidas. Laespecificación 3GPP TS 33.501 destaca la importancia de un proceso de gestión de parches bien definido, que incluya la identificación, evaluación, priorización y despliegue rápido de actualizaciones de seguridad.

Gestión de Configuraciones La configuración segura y la gestión de la infraestructura de red son aspectos críticos para prevenir errores que puedan ser explotados por atacantes. La especificación recomienda la implementación de políticas de configuración estrictas y la automatización de procesos de gestión de configuraciones para minimizar el riesgo de errores humanos.

Estrategias Reactivas de Respuesta

Planificación de Respuesta a Incidentes Desarrollar y mantener un plan de respuesta a incidentes que detalle cómo la organización responderá a los incidentes de ciberseguridad, incluyendo la identificación, contención y erradicación de la amenaza, así como la recuperación de los sistemas afectados (ISO/IEC 27035-1, 2016).

Análisis Forense, realizar análisis forense después de un incidente de seguridad para determinar cómo ocurrió el ataque, la extensión del daño y cómo prevenir incidentes futuros (ACSC, 2020). Comunicación y Notificación de Incidentes Establecer procedimientos para comunicar y notificar incidentes de seguridad a las partes interesadas internas y externas, incluyendo autoridades reguladoras y afectados (GDPR, 2018).

Figura 9

Prácticas de Seguridad

Práctica de Seguridad	Descripción	Tecnología Propuesta	Implementación Propuesta
Cifrado de extremo a extremo (E2EE)	Protección de datos en tránsito y reposo	Algoritmos de cifrado AES-256	Implementación en todos los niveles de comunicación y almacenamiento de datos
Autenticación robusta	Verificación de la identidad de usuarios y dispositivos	Autenticación multifactor (MFA), certificados digitales	Uso de MFA en acceso a sistemas críticos, implementación de PKI para la gestión de certificados
Segmentación de red (Network Slicing)	Creación de múltiples redes virtuales independientes	Tecnologías de virtualización de redes (NFV, SDN)	Configuración de slices de red con políticas de seguridad específicas para cada segmento
Monitoreo y detección de amenazas	Identificación y respuesta en tiempo real a actividades sospechosas	Sistemas de detección y prevención de intrusiones (IDS/IPS), inteligencia artificial (IA)	Implementación de IDS/IPS avanzados, uso de IA para análisis de patrones de tráfico y detección de anomalías
Gestión de identidades y accesos (IAM)	Control de acceso basado en roles y permisos	Soluciones IAM, autenticación federada	Implementación de IAM para gestionar permisos y roles, integración con servicios de autenticación federada
Integridad de la cadena de suministro	Aseguramiento de componentes y software desde la fuente hasta la implementación	Blockchain para trazabilidad y verificación	Uso de blockchain para registrar y verificar transacciones en la cadena de suministro

Nota. Elaboracion propia se identifican prácticas de seguridad de acuerdo con la tecnología y la implementación a realizar Merchan, John (2024)

Herramientas y Tecnologías

Para mejorar la seguridad en las redes 5G, se pueden emplear una variedad de herramientas y tecnologías diseñadas específicamente para abordar los desafíos únicos que presenta esta nueva generación de redes. Estas herramientas y tecnologías cubren aspectos críticos como la protección de la red, la seguridad de los datos y la gestión de identidades y accesos.

Firewalls de Próxima Generación (NGFW), los NGFW proporcionan una capa de seguridad que puede inspeccionar y filtrar el tráfico de red basándose en aplicaciones específicasy protocolos en el nivel de aplicación. Estos firewalls son cruciales para proteger las redes 5G contra accesos no autorizados y ataques maliciosos (Palo Alto Networks, 2020).

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS), estos sistemas monitoreanel tráfico de red en busca de actividades sospechosas que puedan indicar un ataque. Los IPS, en particular, pueden tomar medidas proactivas para bloquear el tráfico malicioso antes de que cause daño (Cisco, 2020).

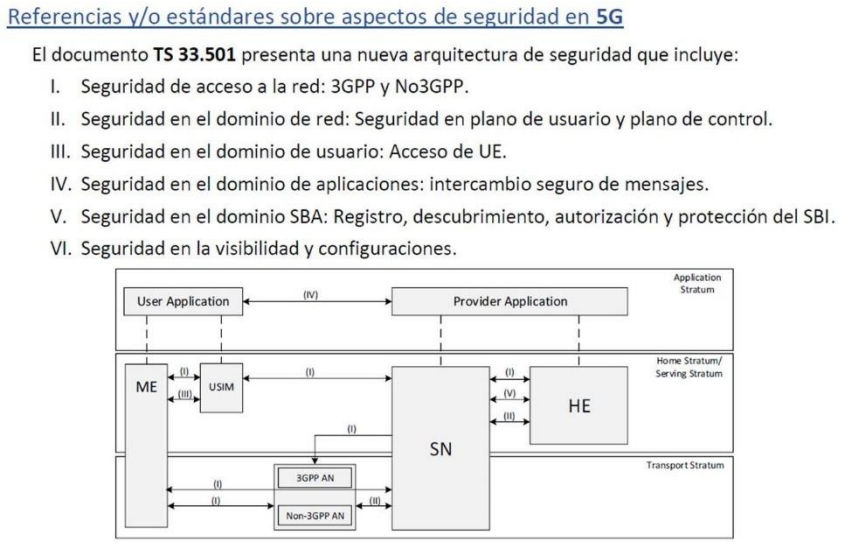
Cifrado de Extremo a Extremo (E2EE), el E2EE asegura que los datos se cifran en el dispositivo de origen y solo se descifran en el dispositivo de destino. Esto impide que los datos sean interceptados y leídos durante la transmisión, proporcionando una fuerte confidencialidad de los datos en las redes 5G (GSMA, 2019).

Gestión de Identidades y Accesos (IAM), las soluciones IAM garantizan que solo los usuarios y dispositivos autenticados puedan acceder a recursos de la red 5G. Esto incluye tecnologías como la autenticación multifactor (MFA) y la gestión de privilegios de acceso (Okta,2021).

Tecnologías de Cadena de Bloques La cadena de bloques puede ser utilizada para mejorar la seguridad en redes 5G, especialmente en la gestión de identidades y la integridad de los datos. La naturaleza descentralizada e inmutable de la cadena de bloques la hace ideal para proteger contra la falsificación y asegurar transacciones y comunicaciones seguras (IBM, 2020). Seguridad Basada en la Nube y Funciones de Red Virtualizada (NFV) La seguridad basada en la nube permite una implementación flexible y escalable de medidas de seguridad,mientras que la NFV facilita la creación de redes virtuales seguras y aisladas dentro de la infraestructura de 5G (VMware, 2020).

Figura 10

Referencias y/o Estándares sobre Aspectos de Seguridad en 5G



Nota. Aspectos de seguridad en 5G Adaptado de *Corletti Estrada, A. (2020). Ciclo de Webinars sobre 5G Presentación e introducción a 5G*. Recuperado de https://www.youtube.com/watch?v=0m9e0mpp2zo&list=PL0QSAEWH0x_hXbHJGO7EPg2iy0gQmU1Tn&index=1

Seguridad de acceso a la red (I), incluye medidas tanto para 3GPP como No3GPP. Seguridad en el dominio de red (II), abarca la seguridad en el plano de usuario y control.Seguridad en el dominio de usuario (III) Se refiere al acceso de UE.

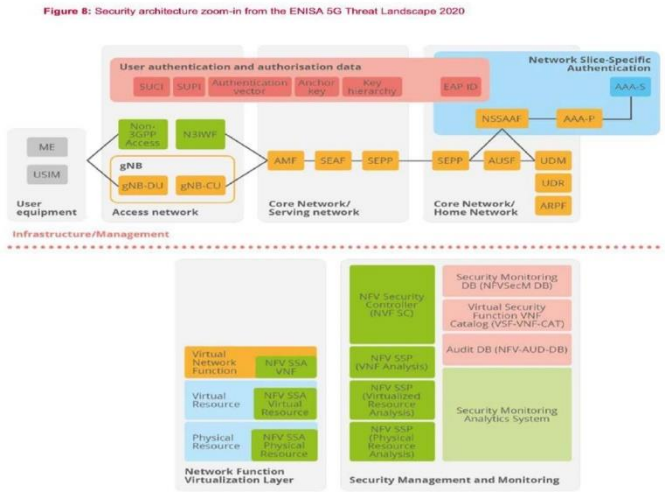
Seguridad en el dominio de aplicaciones (IV) Asegura el intercambio seguro demensajes.

Seguridad en el dominio SBA (V) Cubre registro, descubrimiento, autorización y del SBI.

Seguridad en la visibilidad y configuraciones (VI) Asegura visibilidad y configuraciones adecuadas.

Figura 11

Arquitectura de Seguridad



Nota. Se muestra la arquitectura según ENISA Adaptado de *Corletti Estrada, A. (2020). Ciclo deWebinars sobre 5G: Presentación e introducción a 5G*. Recuperado de https://www.youtube.com/watch?v=0m9e0mpp2zo&list=PL0QSAEWH0x_hXbHJGO7EPg2iy0gQmU1Tn&index=1

Se detalla la arquitectura de seguridad en redes 5G, mostrando cómo diferentes componentes interactúan para proporcionar un entorno seguro. Incluye elementos como la autenticación de usuarios y la gestión de acceso a través de infraestructuras de red virtualizadas yfunciones de red específicas.

Autenticación y autorización de usuarios Utiliza SUCI, SUPI y vectores deautenticación.

Red de acceso (gNB) Se divide en acceso no-3GPP y 3GPP con componentes como N3IWF, gNB-DU y gNB-CU.

Core Network/Serving Network Involucra SEAF, SEPP, AUSF, UDM, y otros. Capa de virtualización de funciones de red Incluye funciones como NFV SSA VNF,

NFV SSA Virtual Resource, y Security Monitoring Analytics System.

Marco Normativo y Regulatorio

Legislación

La legislación que regula la ciberseguridad en las redes 5G varía significativamente entrediferentes países y regiones, reflejando las preocupaciones específicas de seguridad nacional, protección de datos personales y la integridad de las infraestructuras críticas. A continuación, se destacan algunas legislaciones y esfuerzos regulatorios clave a nivel global.

Reglamento General de Protección de Datos (GDPR) de la Unión Europea Aunque no es específico de 5G, el GDPR es fundamental para la ciberseguridad al establecer estrictos requisitos de protección de datos para todas las empresas que operan en la UE, lo que afecta la manera en que los datos personales se manejan dentro de las redes 5G.

Fuente: Unión Europea, GDPR, 2016.

Ley de Ciberseguridad de China Esta legislación establece un marco para la ciberseguridad y la protección de datos, imponiendo requisitos de seguridad para operadores de infraestructuras críticas, lo que incluye redes de telecomunicaciones como 5G.

Fuente: Asamblea Popular Nacional de China, Ley de Ciberseguridad, 2017.Ley de Autorización de Defensa Nacional (NDAA) de los Estados Unidos

Específicamente, las ediciones de 2018 y 2019 de la NDAA incluyen disposiciones relacionadascon la seguridad de las telecomunicaciones y la prohibición del uso de equipos de telecomunicaciones fabricados por ciertas empresas consideradas como riesgos de seguridad nacional para los sistemas 5G en EE.UU.

Fuente: Congreso de los Estados Unidos, NDAA, 2018/2019.

Código Europeo de Comunicaciones Electrónicas (EECC) Aunque abarca una amplia gama de aspectos de las telecomunicaciones, el EECC introduce importantes consideraciones sobre la seguridad y la integridad de las redes, aplicables a la implementación de 5G.

Fuente: Unión Europea, Código Europeo de Comunicaciones Electrónicas, 2018.

Estándares y protocolos

Los estándares y protocolos internacionales juegan un papel crucial en la ciberseguridad de las redes 5G, estableciendo guías y requisitos técnicos que aseguran la protección de la infraestructura, los datos y la privacidad de los usuarios. Varios organismos internacionales han desarrollado estándares específicos para abordar los desafíos de seguridad en el entorno 5G:

Figura 12

Estandares y Protocolos

Organización	Descripción	Estándares y Directrices	Enlace
3rd Generation Partnership Project (3GPP)	3GPP es una colaboración entre grupos de asociaciones de telecomunicaciones que definen los estándares globales para la tecnología móvil, incluido el 5G.	3GPP TS 33.501: Seguridad para Redes 5G	3GPP
Internet Engineering Task Force (IETF)	El IETF desarrolla y promociona protocolos de Internet voluntarios e internacionales que aseguran la operatividad y seguridad de la red.	Protocolos de seguridad IP y de la capa de transporte	IETF
Global System for Mobile Communications Association (GSMA)	La GSMA representa los intereses de los operadores móviles en todo el mundo y desarrolla directrices de seguridad para redes móviles.	Guías y marcos de seguridad para redes móviles 5G	GSMA
Institute of Electrical and Electronics Engineers (IEEE)	IEEE es una organización profesional técnica dedicada a avanzar en la tecnología en beneficio de la humanidad.	Estándares de ciberseguridad para tecnologías de comunicación 5G	IEEE
International Telecommunicatio n Union (ITU)	La ITU es una agencia especializada de las Naciones Unidas que facilita la cooperación internacional en el ámbito de las telecomunicaciones y las TIC.	Estándares globales de seguridad para 5G	ITU
European Union Agency for Cybersecurity (ENISA)	ENISA es una agencia de la Unión Europea que trabaja para mejorar la ciberseguridad en Europa.	Informes y guías sobre ciberseguridad en redes 5G	ENISA
National Institute of Standards and Technology (NIST)	NIST es una agencia del Departamento de Comercio de EE. UU. que desarrolla estándares y directrices para la tecnología y la ciberseguridad.	NIST SP 800-53: Controles de Seguridad y Privacidad	NIST

Nota. Con esta imagen se identifican cada uno de los estándares y que grupos trabajan para establecer normas y estándares de 5G Adaptación propia Elaborado por Merchan, John (2024)

Colaboración Internacional y Gobernanza

En el contexto de las redes 5G, la colaboración internacional y una gobernanza efectiva son esenciales para enfrentar los desafíos de ciberseguridad. Este capítulo explora cómo diferentes organizaciones internacionales contribuyen al establecimiento de estándares, directrices y marcos de trabajo que aseguran las redes, los datos y las comunicaciones en 5G. Además, se discuten los esfuerzos colaborativos que son fundamentales para mitigar los riesgos y asegurar la resiliencia de las infraestructuras de 5G a nivel global.

Organizaciones Internacionales y Estándares

Varias organizaciones internacionales juegan un papel fundamental en la ciberseguridad de 5G, estableciendo estándares, directrices y marcos de trabajo para asegurar las redes, los datosy las comunicaciones. A continuación, se describen algunas de estas organizaciones y su contribución a la ciberseguridad en el ámbito del 5G.

Esfuerzos de Colaboración

La colaboración entre países y empresas es fundamental para asegurar las redes 5G, ya que los desafíos de ciberseguridad que plantea esta tecnología trascienden fronteras y sectores. La naturaleza global de las amenazas cibernéticas, junto con la interconexión inherente a las redes 5G, requiere un enfoque unificado y cooperativo. Aquí se discute la importancia de dicha colaboración.

Compartir Información sobre Amenazas

Importancia Facilita el intercambio de información crítica sobre amenazas cibernéticas emergentes y vulnerabilidades. Esto permite a países y empresas anticipar y prepararse mejor contra ataques, mejorando la resiliencia de las redes 5G globales (ENISA, 2020).

Desarrollo de Estándares de Seguridad Comunes

Importancia Promueve la interoperabilidad y asegura que las redes sean robustas frente a ataques, independientemente de su ubicación geográfica (3GPP, 2020).

Innovación en Soluciones de Seguridad

Importancia Potencia la innovación en soluciones de ciberseguridad para 5G mediante la colaboración entre el sector público y privado (GSMA, 2019).

Respuestas Coordinadas a Incidentes

Importancia Permite una respuesta más rápida y efectiva ante incidentes de seguridad mediante la coordinación de esfuerzos a nivel internacional (ITU, 2020).

Fomentar la Confianza

Importancia Fortalece la confianza entre los stakeholders de 5G mediante la creación de marcos de cooperación transparentes y efectivos (NIST, 2020).

Estudio de Casos y Mejores Prácticas

En el ámbito de la ciberseguridad en redes 5G, los estudios de caso y las mejores prácticas proporcionan valiosas lecciones y estrategias para enfrentar los desafíos únicos que presenta esta tecnología. Este capítulo explora proyectos destacados y las mejores prácticas recomendadas por expertos y organizaciones líderes para asegurar las redes 5G. La información presentada aquí complementa y refuerza los conceptos discutidos en los capítulos anteriores sobre desafíos y estrategias de ciberseguridad.

Estudios de Caso

Uno de los proyectos destacados en este contexto es el emprendido por el National Cybersecurity Center of Excellence (NCCoE) del NIST, centrado en la preparación de una evolución segura hacia el 5G. Este proyecto identifica varios escenarios de uso de 5G y demuestra cómo fortalecer los componentes de la arquitectura 5G para mitigar riesgos identificados y cumplir con los requisitos de cumplimiento de diferentes sectores industriales. Seemplea un enfoque por fases para alinear con el ritmo de desarrollo de la tecnología 5G y la disponibilidad de tecnología comercial 5G, mostrando cómo los productos comerciales y de código abierto pueden aprovechar los estándares de ciberseguridad y las prácticas recomendadas para cada uno de los escenarios de uso de 5G .

Otra fuente valiosa de información es proporcionada por ISACA, que resalta la transformación que 5G traerá a diversas áreas de la sociedad, como vehículos autónomos e interacciones dispositivo a dispositivo. Este análisis detalla cómo la arquitectura abierta y adaptable de 5G, que incluye tecnologías como SDN, IoT, la nube y la virtualización, requiere un enfoque alterado para diseñar políticas de ciberseguridad, estándares, procedimientos, y guías.Se señala que el avance de 5G exigirá un desarrollo de controles de seguridad de un modo

más proactivo y versátil, subrayando la importancia de la autenticación mutua y la encriptación confiable sin comprometer el rendimiento de 5G. ISACA también enfatiza la colaboración entre organizaciones como el 5GPPP, influenciado por la Comisión Europea y las TIC, en la formulación de estándares de 5G.

Estos estudios resaltan la importancia crítica de incorporar la ciberseguridad en todas las etapas del desarrollo y despliegue de las redes 5G, utilizando un enfoque colaborativo entre diferentes actores, incluyendo agencias gubernamentales, operadores de redes móviles, proveedores de servicios y la comunidad académica. La adaptación y aplicación de las leccionesaprendidas en estos proyectos pueden ayudar significativamente a mejorar la resiliencia y seguridad de las infraestructuras 5G en todo el mundo.

Explorando implementaciones exitosas de ciberseguridad en 5G, ABI Research destaca tres estudios de caso en la región Asia-Pacífico.

Swoop Aero en Australia Utiliza drones alimentados por IA y 5G para entregas médicas, aprovechando la comunicación de baja latencia ultrarreliable (URLLC) para operaciones segurasy eficientes (Saunders, J. 2023, Enero 6).

LG Smart Park en Corea del Sur Este parque industrial se ha convertido en una "Fábrica Faro" gracias a IoT, big data, IA y automatización potenciadas por 5G, optimizando la cadena de suministro y los procesos de manufactura (Saunders, J. 2023, Enero 6).

Qingdao Smart Grid en China Implementa una red eléctrica inteligente que utiliza 5G para detectar y solucionar problemas de distribución de energía en milisegundos, mejorando la eficiencia y reduciendo el impacto ambiental (Saunders, J. 2023, Enero 6).

Estos casos ilustran cómo la tecnología 5G puede impulsar la transformación digital en diversos sectores, resaltando la importancia de soluciones innovadoras de ciberseguridad. Para

detalles adicionales sobre estrategias y mejores prácticas implementadas en estos casos, refiérasea las secciones de implementación y mejores prácticas discutidas en los capítulos anteriores sobre estrategias de mitigación y protección (Capítulos 5 y 6).

Mejores Prácticas

Para asegurar las redes 5G, expertos y organizaciones líderes recomiendan varias mejoresprácticas. Estas prácticas complementan las estrategias de mitigación y protección discutidas en el Capítulo 5.

Adoptar un Enfoque de Seguridad por Diseño Integrar consideraciones de seguridad desde las fases iniciales del desarrollo de la red 5G. (Referirse a la sección 5.5 sobre Principios de Diseño Seguro).

Implementar Cifrado de Extremo a Extremo Proteger los datos en tránsito para garantizar su confidencialidad e integridad. (Ver detalles en la sección 5.6 sobre Políticas deCifrado Avanzadas).

Usar Autenticación Fuerte Aplicar mecanismos de autenticación robustos para usuarios ydispositivos. (Referirse a la sección 5.6 sobre Autenticación Multifactor).

Actualizar y Parchear Regularmente Mantener el software y el firmware actualizados para proteger contra vulnerabilidades conocidas. (Ver sección 5.6 sobre Actualizaciones y Gestión de Parches).

Realizar Pruebas de Penetración y Auditorías de Seguridad Evaluar proactivamente la infraestructura 5G contra posibles ataques. (Referirse a la sección 5.6 sobre Monitoreo y Detección de Amenazas).

Estas prácticas están respaldadas por organizaciones como el 3GPP, la GSMA, y el NIST, quienes proporcionan guías y estándares específicos para la seguridad en redes 5G. La

implementación de estas mejores prácticas asegura que las redes 5G sean seguras y resilientesfrente a las amenazas cibernéticas.

Desafíos y Perspectivas Futuras Interoperabilidad y Estandarización

Según Andrews et al. (2014), establecer estándares claros y fomentar la interoperabilidadentre diferentes tecnologías y dispositivos es crucial para el éxito de 5G y futuras generaciones como 6G. Bhutta et al. (2017) también discuten la importancia de los estándares en el desarrollo de redes de próxima generación, destacando la necesidad de un enfoque coordinado para asegurar la interoperabilidad global. Este tema complementa la discusión en el Capítulo 7 sobre la colaboración internacional y la gobernanza, donde se enfatiza la importancia de los estándaresglobales y la interoperabilidad para la seguridad y eficiencia de las redes 5G (ver Sección 7.2).

Inversión en Infraestructura

Rappaport et al. (2013) enfatizan la necesidad de una inversión significativa en infraestructura para la implementación exitosa de tecnologías de comunicación de próxima generación. Esto incluye la expansión de la infraestructura existente y la exploración de nuevas formas de conectividad, como las redes de malla y los satélites en órbita baja, para garantizar unacobertura amplia y fiable. Este tema se conecta con las discusiones en los Capítulos 5 y 6 sobre la importancia de la infraestructura robusta y las mejores prácticas de implementación para asegurar las redes 5G (ver Sección 6.2).

Seguridad y Privacidad

La seguridad cibernética y la protección de la privacidad son aspectos críticos que deben ser integrados desde el principio del desarrollo de 6G para proteger contra amenazas emergentes.Bhutta et al. (2017) señalan la importancia de incorporar medidas de seguridad

avanzadas y estrategias de mitigación para asegurar que las redes futuras sean resilientes frente a ciberataques. Este tema refuerza los conceptos discutidos en los Capítulos 5 y 6 sobre estrategiasde mitigación y protección en redes 5G (ver Secciones 5.6 y 6.3).

Eficiencia Energética

Con el aumento del número de dispositivos conectados, la eficiencia energética se vuelvecada vez más importante. Rappaport et al. (2013) argumentan que para garantizar que 6G sea sostenible desde el punto de vista energético, se necesitan tecnologías y políticas que promuevanla eficiencia energética. Bhutta et al. (2017) destacan la importancia de desarrollar soluciones innovadoras que minimicen el consumo de energía sin comprometer el rendimiento. Este tema complementa las discusiones sobre la sostenibilidad y el impacto ambiental en el Capítulo 6 (verSección 6.4).

Integración de Tecnologías Emergentes

La integración de tecnologías emergentes como la inteligencia artificial y la computacióncuántica será fundamental para 6G. Andrews et al. (2014) mencionan que aprender de las experiencias de implementación de estas tecnologías en 5G puede guiar su integración efectiva en el desarrollo de 6G, potenciando capacidades avanzadas y mejorando la eficiencia operativa. Este tema se alinea con la discusión en el Capítulo 8 sobre la integración de tecnologías emergentes en la implementación de redes 5G (ver Sección 8.2).

Consideraciones Éticas y Sociales

Además de los aspectos técnicos, es importante considerar las implicaciones éticas y sociales de 6G. Bhutta et al. (2017) discuten aspectos como la equidad en el acceso a la tecnología y la protección de datos personales, subrayando la necesidad de abordar estos temas para asegurar que los beneficios de 6G sean accesibles a todos y que la privacidad de los

usuarios esté protegida. Este tema complementa la discusión en el Capítulo 7 sobre la gobernanza y la colaboración internacional (ver Sección 7.3).

Innovación en Ciberseguridad

Las futuras innovaciones en ciberseguridad para 5G y 6G podrían incluir el uso avanzado de inteligencia artificial y aprendizaje automático para anticipar y neutralizar amenazas en tiempo real, la implementación de tecnologías de blockchain para mejorar la integridad y la transparencia de las transacciones, y el desarrollo de sistemas de criptografía cuántica para proteger contra la capacidad de descifrado de las futuras computadoras cuánticas. Estas tecnologías tienen el potencial de fortalecer significativamente la seguridad de las redes 5G y 6G, haciendo que sean más resilientes ante ataques sofisticados y adaptándose dinámicamente a nuevas vulnerabilidades. Este tema refuerza y amplía la discusión sobre estrategias de mitigacióny protección en el Capítulo 5 (ver Sección 5.6).

Conclusiones

La transición hacia las redes 5G marca un hito significativo en la evolución de las telecomunicaciones, prometiendo revolucionar la forma en que interactuamos con el mundo digital y habilitando una nueva generación de aplicaciones y servicios críticos. Sin embargo, esta evolución también trae consigo desafíos de seguridad sin precedentes, impulsados por una mayorsuperficie de ataque, la complejidad de la red y la diversidad de aplicaciones soportadas.

Las estrategias de ciberseguridad propuestas en esta monografía, basadas en la especificación 3GPP TS 33.501, son fundamentales para mitigar los riesgos inherentes a las redes 5G. Estas estrategias incluyen prácticas avanzadas como el cifrado de extremo a extremo (E2EE), la autenticación multifactor (MFA), y la segmentación de red (Network Slicing), que aseguran la confidencialidad, integridad y disponibilidad de los datos. La adopción de estas medidas garantiza que las redes 5G puedan operar de manera segura y eficiente, protegiendo tanto la infraestructura como los datos sensibles de los usuarios.

El análisis detallado de la arquitectura 5G ha revelado varias vulnerabilidades clave, incluyendo una superficie de ataque ampliada debido a la densificación de dispositivos IoT, riesgos asociados con la virtualización y la segmentación de red, y desafíos en la seguridad de la interfaz aérea. Estas vulnerabilidades son críticas y deben ser abordadas para garantizar la seguridad de las redes 5G. La identificación de estas amenazas proporciona una base sólida para desarrollar estrategias de mitigación efectivas.

La evaluación de las directrices y estrategias propuestas por organismos líderes como la GSMA, 3GPP, ENISA y NIST ha sido esencial para comprender las mejores prácticas en ciberseguridad para redes 5G. Estas organizaciones han proporcionado marcos detallados para laimplementación de medidas de seguridad, incluyendo políticas de cifrado, autenticación y

gestión de accesos, y estrategias de mitigación de riesgos. La adopción de estas directricesasegura que las prácticas de seguridad sean coherentes y efectivas a nivel global.

Las propuestas de implementación detalladas en esta monografía, basadas en los lineamientos de la 3GPP TS 33.501, están diseñadas para fortalecer la seguridad de las redes 5G. Estas propuestas incluyen el uso de cifrado de extremo a extremo para proteger los datos en tránsito, la autenticación multifactor para asegurar la identidad de los usuarios y dispositivos, y lasegmentación de red para aislar y proteger diferentes segmentos de la red. Estas medidas no solo cumplen con los estándares internacionales, sino que también adoptan enfoques innovadores paraenfrentar las amenazas actuales y emergentes.

A lo largo de este estudio, se ha demostrado que la seguridad en redes 5G requiere un enfoque integral que combine las mejores prácticas de ciberseguridad con innovaciones tecnológicas avanzadas. Las estrategias y propuestas presentadas en esta monografía no solo cumplen con los lineamientos de la 3GPP TS 33.501, sino que también abordan de manera proactiva las vulnerabilidades identificadas en la arquitectura 5G. La implementación de estas prácticas permitirá a las organizaciones aprovechar las ventajas de la tecnología 5G de manera segura y eficiente.

Para asegurar las redes 5G, es fundamental la colaboración continua entre operadores de redes, proveedores de tecnología, reguladores y la comunidad de seguridad. A medida que avanzamos hacia la adopción masiva de 5G y la evolución hacia 6G, las lecciones aprendidas y las estrategias implementadas servirán como base para futuras innovaciones en la seguridad de redes móviles. Esta colaboración garantizará que las infraestructuras críticas de telecomunicaciones puedan soportar de manera segura el creciente peso de nuestra sociedad

digital, asegurando la resiliencia y protección frente a un panorama de amenazas en constante evolución.

Cronograma y Actividades

Figura 13

Plan de Trabajo

1. PLAN DE TRABAJO												
ACTIVIDAD	**MES 1**	**MES 2**	**MES 3**	**MES 4**	**MES 5**	**MES 6**	**MES 7**	**MES 8**	**MES 9**	**MES 10**	**MES 11**	**MES 12**
Preparación y Planificación	x											
Investigación y Recolección de Datos		X										
Desarrollo del Marco Teórico			x									
Redacción y Análisis				x								
Redacción Final y Revisión					x							
Finalización y Presentación						x						

Nota. Plan de trabajo Cronograma de la monografía elaboración propia Merchan, John (2024)

Mes 1: Preparación y Planificación

Semana 1: Selección del tema y definición del alcance de la monografía.Semana 2: Revisión inicial de literatura y fuentes relevantes.

Semana 3: Elaboración del plan de trabajo detallado y establecimiento de objetivos.

Semana 4: Redacción del esquema preliminar de la monografía y revisión de los métodosde investigación.

Mes 2: Investigación y Recolección de Datos

Semana 5-6: Investigación intensiva y recolección de datos sobre seguridad en redes NGN móviles 5G.

Semana 7: Análisis preliminar de los datos recogidos. Semana 8: Consultas con expertos o asesores si es necesario.

Mes 3: Desarrollo del Marco Teórico

Semana 9-10: Redacción del marco teórico y conceptual.

Semana 11: Integración del marco teórico con la investigación realizada.Semana 12: Primera revisión y edición del marco teórico.

Mes 4: Redacción y Análisis

Semana 13-14: Redacción de los hallazgos y análisis. Semana 15: Desarrollo de los argumentos y discusión.Semana 16: Segunda revisión y edición del borrador. Mes 5: Redacción Final y Revisión

Semana 17-18: Redacción de las conclusiones y recomendaciones. Semana 19: Revisión integral del borrador completo de la monografía.Semana 20: Realización de ajustes y mejoras según sea necesario.

Mes 6: Finalización y Presentación

Semana 21: Revisión final y preparación para la presentación.

Semana 22: Preparación de material de apoyo para la presentación (diapositivas, gráficos,

etc.).

Semana 23: Ensayos de la presentación.

Semana 24: Presentación de la monografía y entrega final.

Presupuesto

El presupuesto para el proyecto de investigación cubrirá los siguientes elementos

Figura 14

Presupuesto

ITEM	**VALOR**
Acceso a Bases de Datos y Literatura Especializada: $0 COP	$0 COP
Suscripciones a journals académicos y bases dedatos especializadas.	$0 COP
Software de Análisis Cualitativo:	$80000 COP
Materiales de Oficina y Gastos Misceláneos: COP	$ 5.000
Incluye impresiones, fotocopias, y otros materialesnecesarios para la investigación.	$0 COP
Honorarios para Revisión Externa: $20000 COP	$20000 COP
Consulta con expertos en ciberseguridadpara revisión del informe final.	$0 COP
Presupuesto Total Estimado:	$105,000 COP

Nota. Presupuesto Elaboracion propia Merchan, John (2024)

Referencias

3rd Generation Partnership Project (3GPP). (2020). *5G security; Specification of the security architecture*. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf

Australian Cyber Security Centre (ACSC). (2020). *Australian Cyber Security Centre incident response. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf?trk=public_post_comment-text*

Akhoundi, M. A., Mousavi, P., & Momeni, M. (2013). *An introduction to 5G: The next generation of mobile communication. 2nd National Conference on Information Technology, Computer, and Telecommunication.*

Ala, Y., et al. (2020). *A comprehensive guide to 5G security. Wiley.*

Al-Dulaimi, A., Wang, X., & Chih-Lin, I. (2015). *5G networks: Fundamental requirements, enabling technologies, and operations management. Wiley.*

Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). *What will 5G be? IEEE Journal on Selected Areas in Communications,* 32(6), 1065-1082.

Buzzi, S., Chih-Lin, I., Klein, T. E., Poor, H. V., Yang, C., & Zappone, A. (2016). *A survey of energy-efficient techniques for 5G networks and challenges ahead.* IEEE Journal on Selected Areas in Communications, 34(4), 697-709.

Chowdhury, M. Z., Shahjalal, M., Ahmed, S., & Jang, Y. M. (2020). *6G wireless communicationsystems: Applications, requirements, technologies, challenges, and research directions*.

IEEE Open Journal of the Communications Society, 1, 957-975.

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *5G security and resilience*.

Disponible en: https://www.cisa.gov/5g-security-and-resilienceCisco. (2020). Intrusion detection and prevention systems (IDPS).

European Union Agency for Cybersecurity (ENISA). (2019). *Threat landscape for 5G networks*.European Union Agency for Cybersecurity (ENISA). (2020). ENISA *threat landscape 2020*.

Forsberg, D., Horn, G., Moeller, W., & Niemi, V. (2007). *LTE security*. John Wiley & Sons.

European Union (EU). (2018). *General Data Protection Regulation* (EU) 2016/679.

Gkagkas, G., Vergados, D. J., Michalas, A., & Dossis, M. (2024). *The advantage of the 5G network for enhancing the Internet of Things and the evolution of the 6G network*. Sensors, 24(8), 2455. https://doi.org/10.3390/s24082455

Global System for Mobile Communications Association (GSMA). (2019). *Understanding end-to-end encryption.*

Global System for Mobile Communications Association (GSMA). (2019). *GSMA mobile security research.*

Global System for Mobile Communications Association (GSMA). (2020). 5G security guidelines.

Huawei. (2021). *Introduction to 5G: Multi-access edge computing*. Recuperado de https://carrier.huawei.com/en/spotlight/5g-mec

IBM. (2020). *Blockchain for enhanced network security*.

ISACA. (n.d.). *5G innovations and cybersecurity risk*. Disponible en: https://www.isaca.org/

International Organization for Standardization (ISO). (2016). *Information technology — Security techniques — Information security incident management* — Part 1: Principles of incident management (ISO/IEC 27035-1).

International Telecommunication Union (ITU). (2020). *Security aspects of 5G system*. Jover, R. P. (2009). *Security attacks against the availability of LTE mobility networks*.

Dissertation, New York University.

Kambourakis, G., Rouskas, A., & Gritzalis, S. (2005). *Securing the UMTS and WCDMA cellularmobile networks. Computer Communications*, 28(9), 986-997.

Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2019). *Edge slicing for 5G networks: Resource allocation and slice embedding*. IEEE Internet of Things Journal.

National Cybersecurity Center of Excellence (NCCoE). (n.d.). *5G cybersecurity*. Disponible en: https://www.nccoe.nist.gov/5g-cybersecurity

National Institute of Standards and Technology (NIST). (2022). *SP 1800-33*, 5G cybersecurity. Disponible en: https://csrc.nist.gov/

National Institute of Standards and Technology (NIST). (2020). *Framework for improving critical infrastructure cybersecurity*.

Okta. (2021). *Identity and access management (IAM) solutions*. Palo Alto Networks. (2020). *Next-generation firewalls (NGFWs*).

Petit, J., Schaub, F., Feiri, M., & Kargl, F. (2015). *Pseudonym schemes in vehicular networks: Asurvey. IEEE Communications Surveys & Tutorials.*

Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., & Taleb, T. (2018). *Survey on multi-access edge computing for Internet of Things realization*. IEEE Communications Surveys& Tutorials.

Saad, W., Bennis, M., & Chen, M. (2020*). A vision of 6G wireless systems: Applications, trends,technologies, and open research problems*. IEEE Network.

Saunders, J. (2023, enero 6). *Enterprise 5G in Asia-Pacific: 3 case studies to help mobile operators assess the world's largest cellular market*. Recuperado de https://www.abiresearch.com/blogs/2023/01/06/5g-in-asia-pacific-case-studies/

VMware. (2020). *Network functions virtualization (NFV) for improved network security*.