# Universidad Nacional de Loja

## Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

### Maestría en Telecomunicaciones

# Análisis comparativo entre la seguridad empleada en redes 4G y redes 5G.

**Trabajo de Titulación, previo a la obtención del título de Magister en Telecomunicaciones.**


**AUTOR:**

Ing. Jandry Dario González González

**DIRECTOR:**

Ing. John Jossimar Tucker Yépez, Mg. Sc.


**Loja – Ecuador**

2024

**Certificación**

Loja, 25 de junio de 2024

Ing. John Jossimar Tucker Yépez, Mg. Sc.
**DIRECTOR DEL TRABAJO DE TITULACIÓN**

**CERTIFICO:**

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis comparativo entre la seguridad empleada en redes 4G y redes 5G,** previo a la obtención del título **de Magíster en Telecomunicaciones,** de la autoría del estudiante **Jandry Darío González González**, con **cédula de identidad Nro. 1105375842,** una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
JOHN JOSSIMAR TUCKER YEPEZ

Ing. John Jossimar Tucker Yépez, Mg. Sc.
**DIRECTOR DEL TRABAJO DE TITULACIÓN**

## Autoría

**Yo, Jandry Darío González González,** declaro ser autor del presente Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.


**Firma:**

**Cédula de Identidad:** 1105375842

**Fecha: 25/06/2024**

**Correo electrónico:** jandry.gonzalez@unl.edu.ec

**Teléfono:** 0992121572

**Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.**

Yo, **Jandry Darío González González**, declaro ser autor del Trabajo de Titulación denominado: **Análisis comparativo entre la seguridad empleada en redes 4G y redes 5G**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, suscribo, en la ciudad de Loja, a los 25 días del mes de junio de dos mil veinticuatro.


Firmado electrónicamente por:
JANDRY DARIO
GONZALEZ GONZALEZ

**Firma:**

**Cédula de identidad**: 1105375842

**Dirección**: Alonzo de Mercadillo y Chile

**Correo Electrónico**: **jandry.gonzalez@unl.edu.ec**

**Teléfono**: 0992121572

**DATOS COMPLEMENTARIOS:**

**DIRECTOR DEL TRABAJO DE TITULACIÓN:** Ing. John Jossimar Tucker Yépez, Mg. Sc.

## Dedicatoria

Este trabajo lo quiero dedicar primeramente a Dios, quien ha sido mi guía y fortaleza, quien ha sido la luz que ha iluminado mi camino desde niño y a lo largo de esta travesía académica para llegar a ser un profesional exitoso. Con humildad y gratitud, reconozco su amor incondicional y la sabiduría que ha derramado sobre mí. Sin su presencia en mi vida, nada de esto hubiera sido posible.

A mis padres quienes siempre han sido esa fuente inagotable de amor, apoyo y aliento incondicional. Gracias por ser mi mayor inspiración y por creer en mí en cada paso que eh dado en esta travesía académica. Su sacrificio, apoyo y dedicación han sido la fuerza impulsora detrás de este logro.

A mis queridos hermanos, quienes me han acompañado en esta travesía con su aliento y palabras de ánimo. Sus deseos y alegrías compartidos han sido mi motivación para superar cualquier obstáculo que se presentara.

Y finalmente, a todos aquellos que de una u otra forma contribuyeron a que este logro se hiciera realidad. Muchas gracias.

***Jandry Dario González González***

**Agradecimiento**

Primeramente, agradezco a Dios por ser el guía en mi vida y a la vez expresar mi profunda gratitud por la sabiduría, fortaleza y perseverancia necesarias para culminar esta etapa académica. Gracias padre celestial por todas las bendiciones derramadas en la travesía de mi vida académica y profesional.

A mis padres y hermanos por ser ese pilar fundamental, puesto que, con sus palabras de aliento y motivación han permitido que hoy logre culminar con mayor éxito mi maestría, sepan que no son únicamente mis logros, sino que también les pertenecen a ustedes.

A mi tutor, el Ing. John Tucker Yépez, Mg. Sc, por estar siempre presente, con sus orientaciones, paciencia y motivación constante, para que este trabajo investigativo llegue a su etapa de culminación.

A todas aquellas personas que fueron parte de este proceso académico que con gran sabiduría se han esforzado por ayudarme a llegar al punto en el que me encuentro hoy.

*¡¡¡Gracias totales!!!*

***Jandry Dario González González***

## Índice de Contenidos

**Índice de Tablas:**

**Índice de Figuras:**

**Índice de Anexos:**

## 1. Título

**Análisis comparativo entre la seguridad empleada en redes 4G y redes 5G.**

## 2. Resumen

Dada la rápida evolución tecnológica y el incremento exponencial en el uso de dispositivos móviles, la seguridad en las redes de comunicación se ha convertido en un aspecto crítico. La tecnología 5G ha traído consigo importantes avances en términos de mayores velocidades de transmisión de datos, menor latencia y capacidad de conexión de dispositivos. Sin embargo, también plantea nuevos desafíos en materia de seguridad en comparación con las redes 4G existentes.

El presente trabajo tiene como objetivo realizar un análisis exhaustivo de las medidas de seguridad implementadas en las redes 4G y 5G, identificando sus fortalezas, debilidades y diferencias clave, evaluando su eficacia frente a amenazas como interceptación de datos, ataques de denegación de servicio y vulnerabilidades de seguridad. Además, se analizan los mecanismos de seguridad implementados para mantener la integridad, disponibilidad y confidencialidad en la comunicación móvil, garantizando la privacidad de los datos de los usuarios. Al mismo tiempo, se evalúan las estrategias de mitigación implementadas y las posibles soluciones de seguridad de las redes 5G, como es la implementación de redes definidas por software (SDR) y la virtualización de funciones de red (NFV) que aseguran una mayor protección de datos.

Finalmente se pretende proporcionar recomendaciones y medias concretas para mejorar la seguridad en las implementaciones de redes 5G y su impacto en la protección de datos y privacidad del usuario, a fin de garantizar una transición segura hacia las redes 5G y proteger la integridad y privacidad de los datos de los usuarios.

***Palabras claves**: Confidencialidad, Seguridad Informática, Privacidad, Vulnerabilidades, Virtualización.*

**Abstract**

Given the rapid technological evolution and the exponential increase in the use of mobile devices, security in communication networks has become a critical issue. 5G technology has brought with it significant advances in terms of higher data transmission speeds, lower latency and device connectivity capabilities. However, it also poses new security challenges compared to existing 4G networks.

This paper aims to perform a comprehensive analysis of the security measures implemented in 4G and 5G networks, identifying their strengths, weaknesses and key differences, assessing their effectiveness against threats such as data interception, denial-of-service attacks and security vulnerabilities. In addition, the security mechanisms implemented to maintain integrity, availability and confidentiality in mobile communication are analyzed, guaranteeing the privacy of user data. At the same time, it evaluates the mitigation strategies implemented and the possible security solutions for 5G networks, such as the implementation of software-defined networks (SDR) and network functions virtualization (NFV) that ensure greater data protection.

Finally, it is intended to provide concrete recommendations and measures to improve security in 5G network implementations and their impact on data protection and user privacy, in order to ensure a secure transition to 5G networks and protect the integrity and privacy of user data.

*Keywords: Confidentiality, Information Security, Privacy, Vulnerabilities, Virtualization.*

## 3. Introducción

El proyecto de investigación tiene como finalidad realizar un análisis comparativo de la seguridad empleada en las redes 4G y 5G. La migración de las redes 4G a las 5G representa una transición tecnológica importante en el ámbito de las telecomunicaciones. Este cambio no solo implica mejoras en la velocidad y capacidad, sino también transformaciones significativas en la arquitectura de red, en las tecnologías subyacentes y la seguridad.

La implementación de redes 5G afecta no solo a las telecomunicaciones, sino también a una variedad de sectores, incluidos el IoT, la salud, la industria automotriz y más. La seguridad de estas redes es crucial para garantizar la integridad, confidencialidad y disponibilidad de datos críticos en estas áreas.

Las redes 5G presentan desafíos únicos en términos de seguridad, como la conectividad masiva de dispositivos y la baja latencia. Comprender y analizar estas características es esencial para abordar los riesgos emergentes y garantizar la robustez de las infraestructuras de comunicación. La seguridad de las redes 4G y 5G está estrechamente ligada a la protección de la privacidad de los usuarios y la confidencialidad de la información transmitida. El análisis comparativo permite evaluar cómo estas nuevas tecnologías abordan estos aspectos críticos.

Dado que la implementación de redes 5G es un fenómeno global, entender las diferencias en las medidas de seguridad entre las generaciones de redes es esencial para empresas, gobiernos y usuarios en todo el mundo.

La seguridad de las redes 5G es un tema de interés público. Un análisis comparativo brinda información accesible y necesaria para aumentar la conciencia pública sobre los riesgos y beneficios asociados con la evolución de las redes de comunicación.

En resumen, el análisis comparativo entre la seguridad en redes 4G y 5G es vital para entender las implicaciones de esta transición tecnológica, asegurar la integridad de la infraestructura de comunicación y prepararse adecuadamente para los desafíos y oportunidades que surgen con las redes 5G.

# Objetivos

## Objetivo general

Analizar las principales amenazas de la seguridad de las redes 5G comparadas con las amenazas que actualmente existen en redes 4g para determinar los desafíos que seguridad que se presentan en ambas tecnologías móviles.

## Objetivos específicos

- Analizar las amenazas de seguridad en redes 5G y 4G para determinar las brechas de seguridad existente entre las tecnologías.

- Evaluar la efectividad de las medidas de seguridad existentes en las redes 5G como la integridad, disponibilidad y la confidencialidad para definir las áreas donde se necesitan mejoras.

- Proponer recomendaciones y medidas concretas para mejorar la seguridad de las redes 5G y garantizar una mejor seguridad de navegación al usuario.

# 4. Marco teórico

En el presente apartado se realizará la revisión bibliográfica afines a la seguridad empleada en las redes móviles 4G y 5G que se debe tener en cuenta para poder analizar la presente investigación.

## 4.1.Seguridad de la Información

La tecnología en la actualidad nos permite ser más productivos y nos permite acceder a una gran cantidad de información con solo dar un click, como trabajar remotamente, acceder a correos electrónicos, realizar compras en línea, verificar nuestro saldo bancario y así sucesivamente con muchos aspectos de nuestra vida cotidiana, pero esto también conlleva a estar expuestos a una cantidad de problemas de seguridad.

La seguridad de la información se define como un conjunto de medidas y controles para proteger la confidencialidad, integridad y disponibilidad de los activos de información, asegurando su tratamiento, gestión y preservación adecuada desde una perspectiva del ciclo de vida completo.

La seguridad de la información abarca múltiples aspectos, como la seguridad de los datos, la seguridad de las aplicaciones, la seguridad de las redes y comunicaciones, la seguridad física y la seguridad de los recursos humanos. Su objetivo principal es minimizar los riesgos y amenazas a los que se enfrentan los activos de información, asegurando la continuidad del negocio y cumpliendo con los requisitos legales, normativos y contractuales aplicables (Muñoz, 2021).

## 4.2.Triada de la seguridad informática

La seguridad de la información debe cumplir con ciertas características para que esta sea eficiente, según la norma ISO 27001 establece tres aspectos fundamentales como:

### *4.2.1. Integridad*

Los sistemas que manejan la información deben asegurarse de que la información sea auténtica, es decir, sin alteraciones o manipulaciones que no hayan sido autorizadas previamente. El objetivo principal es asegurarse de que los datos se transmitan en un entorno seguro utilizando protocolos y técnicas para evitar cualquier riesgo potencial.

### *4.2.2. Confidencialidad*

La confidencialidad garantiza que la información y los datos recopilados solo sean accesibles a las personas o entidades autorizadas y que no se compartan sin el permiso adecuado. Los sistemas de seguridad de la información deben asegurarse de que la confidencialidad de la información nunca se vea comprometida

### *4.2.3. Disponibilidad*

En este sentido, se garantiza que la información esté disponible y accesible en todo momento para todas las personas o entidades autorizadas para su manejo y comprensión. Para lograr esto, se deben implementar medidas de soporte y seguridad para garantizar el acceso a la información cuando sea necesario y prevenir la interrupción de los servicios (Toro, 2021).

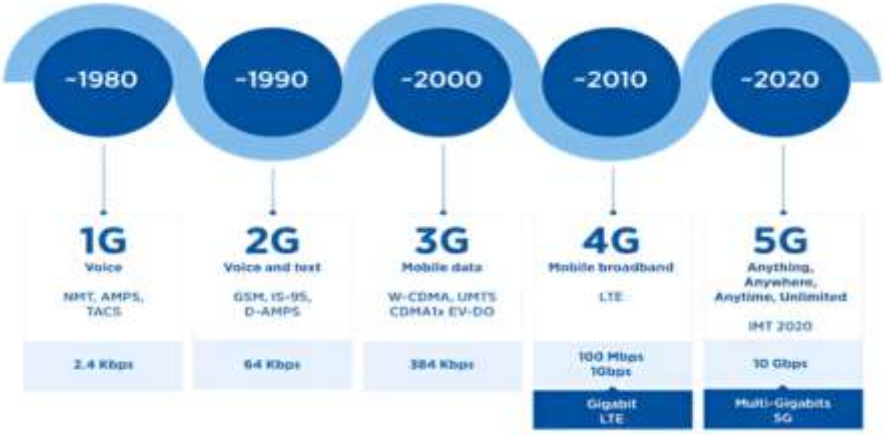
## 4.3.Redes Moviles

Una red móvil consiste en una red de estaciones base que rodean una celda y envían ondas de radio desde y hasta los terminales de los usuarios. El principio general de la telefonía se aplica a las comunicaciones móviles: conectar dos usuarios remotos a través del equipo de red de un operador de gestión del servicio. Sin embargo, la red móvil depende de las transmisiones de radio, a diferencia de los teléfonos fijos, donde no hay pares de cobre ni fibra óptica. La antena o estación base conecta el teléfono móvil del usuario a través del aire con la central del operador, lo que permite dirigir la comunicación hacia el dispositivo correspondiente en la red móvil, fija o a través de otras antenas.

El usuario móvil debe estar dentro del área de cobertura de una antena para que la comunicación sea efectiva. Esta tiene un alcance limitado y cubre una celda, es decir un área pequeña, es por ello el nombre red de celdas o red celular que se usa con frecuencia para referirse a las redes móviles. Los operadores despliegan miles de celdas, cada una equipada con estaciones base, para cubrir el mayor territorio y garantizar que los usuarios puedan llamar siempre, asegurándose de que nunca se pierda la comunicación beneficiándose de los servicios de la red de telefonía móvil (Orange, s. f.).

### 4.4.Evolución de las comunicaciones móviles

**Figura 1**
Evolución de las redes móviles




*Fuente: (Unitec, 2020)*

Un ataque en las últimas décadas, se ha experimentado un notable progreso en las tecnologías de comunicación móvil. A medida que estas tecnologías han ido evolucionando, se ha adoptado la convención de asignarles un número de generación, como 2G, 3G, 4G y 5G. Las primeras redes móviles, conocidas como primera generación, surgieron en la década de 1980 y se basaban principalmente en sistemas analógicos. Posteriormente, la segunda generación (2G) trajo consigo el estándar GSM (Sistema Global para las Comunicaciones Móviles), el cual revolucionó las comunicaciones móviles. Sin embargo, debido a la creciente demanda de conexiones en todo el mundo, los estándares de comunicación móvil continuaron avanzando rápidamente para dar soporte a un mayor número de usuarios, culminando en el actual estándar 5G, que representa la quinta generación de redes móviles (Taipe, 2022).

### 4.5.Redes móviles de primera generación 1G

La primera generación de comunicación móvil comenzó alrededor de 1980 y se basó en la transmisión analógica. Las principales tecnologías utilizadas incluyeron AMPS (Advanced Mobile Phone System) en América del Norte, NMT (Nordic Mobile Telephony) desarrollado por los operadores de redes telefónicas públicas controladas por el gobierno de los países nórdicos y TACS (Total Access Communication System) en el Reino Unido. Los sistemas de comunicación

móvil de primera generación limitaron los servicios de voz y, por primera vez, hicieron que la telefonía móvil fuera accesible para la gente común (Flores Erazo, 2022).

**Figura 2**
Teléfono de primera generación móvil


*Fuente: (Hcordova, 2014)*

Según la (Arcotel, 2020) la tecnología 1G fue la primera red celular que permitió solamente realizar llamadas de voz ya que la transferencia de datos era imposible, a continuación, se describen algunas características de esta red móvil:

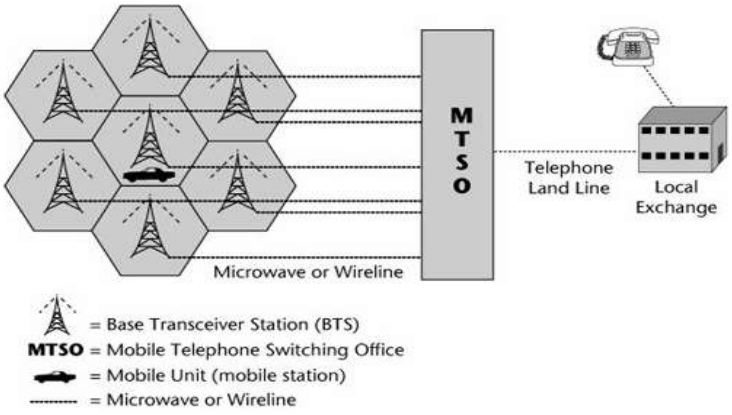
- Año: 1970 - 1980
- Estándares: AMPS (Advanced Mobile Phone System).
- Servicios: Sólo voz y ninguna seguridad ya que las llamadas de vos se producen en las torres de radio.
- Tecnología: analógica
- Velocidad: 1kbps a 2,4 kbps
- Multiplexación: FDMA
- Conmutación: conmutación de circuitos
- Core Network: PSTN Frecuencia: 800 - 900 MH

### *4.5.1. Arquitectura primera generación 1G*

Esta arquitectura posee tres elementos claves; una estación transceptora, una oficina de conmutación de telefonía móvil (MTSO) y una unidad móvil es decir el teléfono del usuario.

**Figura 3**

Arquitectura primera generación




*Fuente: (Flylib, 2020)*

A continuación, se describe cada bloque

- BS: estación base
- MTSO: Oficina de conmutación de telefonía móvil
- Mobile unit: unidad móvil o teléfono

Cada celda requiere una estación transceptora base, que es una torre que transmite señales a la unidad móvil y desde ella. Cada una de estas estaciones transceptoras base está conectada a un MTSO. Para completar las llamadas a través de la PSTN, la MTSO luego interactúa con las centrales locales terrestres. El MTSO y las estaciones transceptoras base pueden conectarse por microondas o por cable. Por lo general, hay una instalación por cable desde el MTSO a la central local, pero también puede ser de microondas.

### 4.6.Redes móviles de segunda generación 2G

La segunda generación (2G) de redes móviles surgió en la década de 1990 y se distinguió por su naturaleza digital, en contraste con la tecnología analógica de la primera generación. El enfoque principal de esta nueva generación era mejorar la calidad de voz, aumentar la capacidad de la red y ampliar la cobertura. Si bien los protocolos 2G permitían velocidades de transmisión de datos más altas para las comunicaciones de voz, las capacidades para la transferencia de datos seguían siendo limitadas. No obstante, estas redes ofrecían servicios auxiliares como el envío de datos, fax y mensajes cortos (SMS). La mayoría de los protocolos 2G incorporaban diferentes

niveles de encriptación para brindar mayor seguridad. En Estados Unidos y otros países, esta generación se conocía como PCS (Servicios de Comunicaciones Personales) (Flores Erazo, 2022).

**Figura 4**

Teléfono móvil de segunda generación


*Fuente: (Hcordova, 2014)*

Según la (Arcotel, 2020) la tecnología GSM (Sistema Global para las Comunicaciones Móviles) fue la primera en facilitar voz y datos en las redes móviles, así como el roaming internacional que permitía a los usuarios mantener conectividad mientras se desplazaban entre diferentes ubicaciones geográficas, a continuación, se describen algunas características de esta red móvil:

- Año: 1980 -1990
- Tecnología: Digital
- Velocidad: 14 Kbps a 64 Kbps
- Banda de frecuencia: 850 - 1900 MHz (GSM) y 825 - 849 MHz (CDMA)
- Ancho de banda / canal: GSM divide cada canal de 200 kHz en bloques de 25 kHz el canal CDMA es nominalmente de 1,23 MHz
- Multiplexación / Tecnología de acceso: TDMA y CDMA.
- Conmutación: Conmutación de circuitos
- Estándares: GSM (Sistema Global para Comunicaciones Móviles), IS-95 (CDMA) - utilizado en América y partes de Asia), JDC (Celular Digital Japonés) (basado en TDMA), utilizado en Japón, iDEN (basado en TDMA), red de comunicación propietaria utilizado por Nextel en los Estados Unidos.
- Servicios: Voz Digital, SMS, roaming internacional, conferencia, llamada en espera, retención de llamada, transferencia de llamadas, bloqueo de llamadas, número de identificación de llamadas, grupos cerrados de usuarios (CUG), servicios USSD, autenticación, facturación basada en los servicios prestados a sus clientes, por

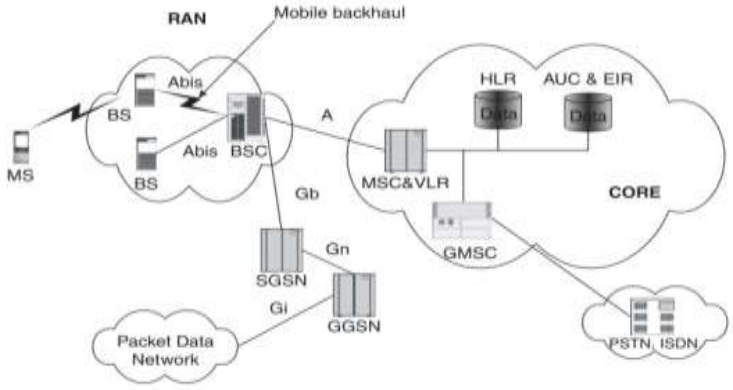
ejemplo, cargos basados en llamadas locales, llamadas de larga distancia, llamadas con descuento, en tiempo real de facturación.

### *4.6.1. Arquitectura segunda generación 2G*

Esta tecnología fue conocida como GSM y aportó una serie de servicios como el roaming global, mensajes de texto SMS, autenticación, cifrado de los datos de usuario y de la señalización, además de la mejora en privacidad del usuario al cifrar su identificador. Se implementó GPRS, el servicio de paquetes de radio de GSM lo que permitió introducir el protocolo IP en los dispositivos, para ello debieron introducirse dos nuevos nodos a la arquitectura, el nodo de servicio GPRS(SGSN) y la puerta de enlace al nodo de soporte GPRS(GGSN).

Su arquitectura se basa en la red de acceso radio (RAN), el núcleo de la red, así como la red de gestión.

**Figura 5**
Arquitectura segunda generación




*Fuente: (Rojo, 2021)*

A continuación, se describe cada bloque:

- MS: Estación móvil
- BS: Estación base
- BSC: Estación base de control
- MSC: Centro de conmutación móvil
- GMSC: Gateway MSC
- HLR: Registro de ubicación local
- VLR: Registro de ubicación de visitante

- AuC: Centro de autenticación
- SGSN: Nodo de soporte de servicio GPRS
- GGSN: Nodo de soporte de puerta de enlace GPRS

El teléfono móvil se conecta mediante aire a la BS y estas están controladas por la BSC y a su vez por el centro de conmutación móvil MSC el cual está conectado a la Red telefónica pública conmutada (PSTN). Si el usuario desea acceder a datos móviles entra en funcionamiento los bloques del nodo de soporte de servicio SGSN y el nodo de soporte de puerta de enlace para comunicarse con la red de paquetes de datos.

### 4.7.Redes móviles de tercera generación 3G

La tercera generación de comunicaciones móviles, comúnmente conocida como 3G, hizo su aparición a principios de la década de 2000. Con 3G se dio el verdadero salto hacia la banda ancha móvil de alta calidad, lo que permitió un acceso rápido a Internet de forma inalámbrica. Este avance fue posible gracias a la evolución 3G denominada HSPA (High Speed Packet Acces). Además, mientras que las tecnologías móviles previas habían sido diseñadas para operar en espectro apareado (con bandas separadas para los enlaces de red a dispositivo y viceversa) basado en duplexación por división de frecuencia (FDD), la generación 3G marcó la primera introducción de comunicaciones móviles en espectro no emparejado, a través de la tecnología TD-SCDMA desarrollada en China, la cual se fundamenta en la duplexación por división de tiempo (TDD)(Oviedo, 2022).

**Figura 6**

Teléfono de tercera generación móvil


*Fuente: (Hcordova, 2014)*

La llegada de esta comunicación dio un gran salto ya que se pasó de la transmisión de llamadas de voz y mensajes de texto a poder navegar por internet desde los teléfonos móviles a

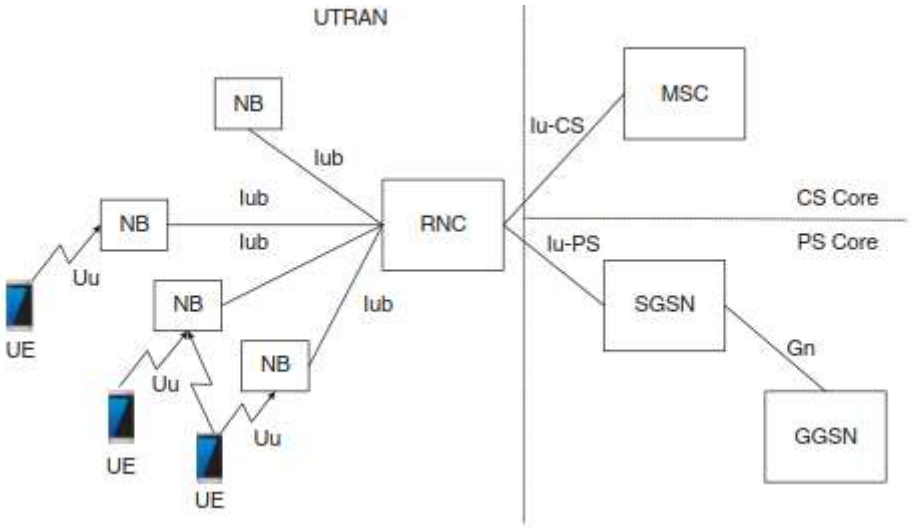
una velocidad bastante alta. La tercera generación de estándares UMTS (Sistema Universal de Telecomunicaciones Móviles) utiliza la tecnología CDMA y ofrece un intercambio de información aproximado de cinco veces más que la tecnología 2G, a continuación, se describen algunas características:

- Año: 2000
- Estándares: UMTS (WCDMA) basado en GSM (Global Systems for Mobile) infraestructura del sistema 2G, estandarizado por el 3GPP y CDMA 2000 basado en la tecnología CDMA (IS-95) estándar 2G, estandarizada por 3GPP2.
- Velocidad: 384 Kbps a 2 Mbps
- Frecuencia: aproximadamente 8 a 2,5 GHz
- Ancho de banda: de 5 a 20 MHz
- Multiplexación / Tecnología de acceso: Interfaz de radio llamada WCDMA (Wideband Code División Multiple Access) HSPA es una actualización de W-CDMA que ofrece velocidades de 14,4 Mbit/s de bajada y 5,76 Mbit/s de subida o HSPA+ puede proporcionar velocidades de datos pico teóricas de hasta 168 Mbit/s de bajada y 22 Mbit/s de subida.
- Servicios: telefonía móvil de voz, acceso y navegación por internet de alta velocidad, llamadas de video, chat y conferencias, servicios basados en la localización, telemedicina, correo electrónico, fax y mapas de navegación, juegos, música móvil, servicios multimedia, como fotos digitales y películas. servicios localizados para acceder a las actualizaciones de tráfico y clima, servicios móviles de oficina, como la banca virtual (Arcotel, 2020).

### *4.7.1. Arquitectura tercera generación 3G*

La tercera generación más conocida con el nombre de Sistema de Telecomunicaciones Móvil Universal (UMTS) implementó la separación entre el plano de control y el plano de usuario, así como la separación de la red radio de la red de transporte. Su arquitectura es similar a GSM aunque ahora en vez de las estaciones base y el controlador evolucionan tomando el nombre de Nodeb y la radio Network Controler(RNC) (Rojo, 2021).

**Figura 7**
Arquitectura de tercera generación




*Fuente: (Rojo, 2021)*

A continuación, se describe cada bloque:

- UE: Equipo de usuario
- Nodo B: Estación base
- RNC: Controlador de red radio
- MSC: Centro de conmutación móvil
- HLR: Registro de ubicación local
- VLR: Registro de ubicación de visitante
- AuC: Centro de autenticación
- SGSN: Nodo de soporte de servicio de datos
- GGSN: Nodo de soporte de puerta de enlace para datos

El acceso radio es conocido como UTRAN el cual está formado por dos elementos de red; el Nodo B que es la estación base que sirve para gestionar las conexiones con los UE que se encuentran en una celda cercana.

### 4.8.Redes móviles de cuarta generación 4G

La cuarta generación (4G) de comunicaciones móviles, representada por la tecnología LTE, se han seguido los pasos de HSPA, brindando una mayor eficiencia y una experiencia mejorada de banda ancha móvil en términos de mayores velocidades de datos alcanzables para el usuario final. Esto se logra mediante la transmisión basada en OFDM, que permite anchos de banda de transmisión más amplios y el uso de tecnologías más avanzadas de múltiples antenas. Además, mientras que la 3G permitió las comunicaciones móviles en espectro no apareado a través de una tecnología de acceso radioeléctrico específica (TD-SCDMA), LTE admite operaciones tanto FDD como TDD, es decir, en espectros apareados y no apareados, dentro de una tecnología común de acceso radioeléctrico. Mediante LTE, el mundo se ha convertido en una única tecnología global para la comunicación móvil, utilizada por prácticamente todos los operadores de redes móviles y aplicable tanto a espectros con licencia como sin licencia (Flores Erazo, 2022)

**Figura 8**
Teléfono móvil de cuarta generación


*Fuente: (Hcordova, 2014)*

La red 4G nos permite navegar por internet, bajar aplicaciones en segundos o jugar en línea sin ningún tipo de retardos, esta son redes móviles de cuarta generación LTE(Long Term Evolution), a continuación, algunas características de esta tecnología (Arcotel, 2020).

- Año: 2010 la UIT-R especifica los requisitos para los sistemas 4G.
- Estándares: Long-Term Evolution Time-Division Duplex (LTE-TDD y LTE-FDD) estándar WiMAX móvil (802.16m estandarizado por el IEEE) Velocidad -

100 Mbps en movimiento y 1 Gbps cuando se permanece inmóvil. Telefonía IP nuevas frecuencias, ancho de banda de canal de frecuencia más amplia.

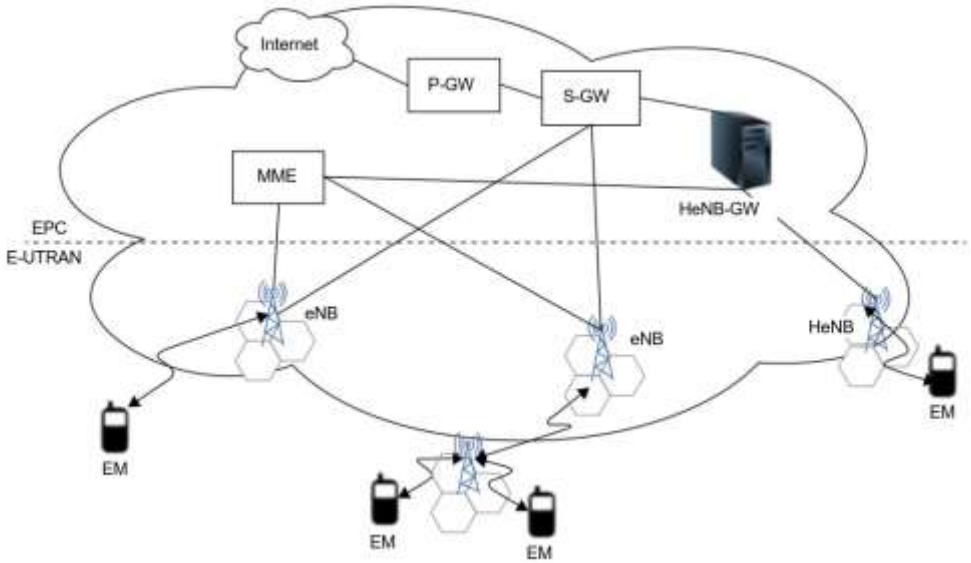
- Tecnologías de multiplexación / acceso: OFDM, MC-CDMA, CDMA y LAS-Red-LMDS
- Ancho de Banda: 5-20 MHz, opcionalmente hasta 40 MHz bandas de frecuencia: - LTE cubre una gama de diferentes bandas. En América del Norte se utilizan 700, 750, 800, 850, 1900, 1700/2100 (AWS), 2300 (WCS) 2500 y 2600 MHz (bandas 2, 4, 5, 7, 12, 13, 17, 25, 26 , 30, 41); 2500 MHz en América del Sur; 700, 800, 900, 1800, 2600 MHz en Europa (bandas 3, 7, 20); 800, 1800 y 2600 MHz en Asia (bandas 1, 3, 5, 7, 8,11, 13, 40) 1800 MHz y 2300 MHz en Australia y Nueva Zelanda (bandas 3, 40).
- Servicios: acceso móvil web, telefonía IP, servicios de juegos, TV móvil de alta definición, videoconferencia, televisión 3D, computación en la nube, gestión de flujos múltiples de difusión y movimientos rápidos de teléfonos móviles, video digital, acceso a información dinámica y dispositivos portátiles.

### *4.8.1. Arquitectura cuarta generación 4G*

Las redes móviles LTE se caracterizan por estar basadas en el protocolo IP, las cuales requieren métodos y técnicas basadas en la conmutación de paquetes. La arquitectura de la red LTE permite la transferencia de paquetes IP entre los terminales de usuario y las redes de paquetes de telecomunicaciones externas, como Internet.

**Figura 9**

Arquitectura cuarta generación




*Fuente: (Adewumi et al., 2020)*

En LTE se divide el sistema entres elementos como es el equipo de usuario (EM), una nueva red de acceso denominada Red de acceso de radio terrestre universal (E-UTRAN) y una red troncal denomina núcleo de paquetes evolucionado (EPC).

La estación base E-UTRAN integra toda la funcionalidad de la red de acceso mediante el Envolved Node (eNB) el cual utiliza los protocolos específicos de la interfaz radio para realizar la transmisión de los paquetes IP hacia el equipo del usuario. La red troncal EPC proporciona el servicio de conectividad IP permitiendo el acceso a redes externas y a plataformas de servicio como IMS. Los elementos principales del EPC son el Mobility Management Entity (MME), el Serving Gateway (S-GW) y el Packet Data Network Gateway(P-GW) que constituyen los elementos principales para la prestación del servicio de conectividad IP entre el equipo de usuario conectado a la red de acceso E-UTRAN y redes externas a las que se conecta la red troncal EPC (Adewumi et al., 2020).

- E-UTRAN: Red de acceso de radio terrestre universal
- EPC: Núcleo de paquetes evolucionado
- EM: Equipo móvil
- eNB: Estación base
- MME: Entidad de gestión de movilidad
- S-GW: Puerta de enlace de servicio

- P-GW: Puerta de enlace de red de datos por paquetes.

### 4.9.Redes Moviles de quinta generación 5G

La tecnología móvil 5G representa la evolución de la generación 4G, y su propósito es innovar nuestras vidas mediante el uso de nuevas redes que permitan potenciar el Internet de las Cosas (IoT), como los vehículos inteligentes, la banda ancha móvil, la visualización de contenidos de alta velocidad con calidad 4K y otros servicios que requieren un uso intensivo del ancho de banda.

Además, la tecnología 5G habilita la navegación por Internet a velocidades de hasta 10 Gbps, diez veces más rápido que los principales servicios de fibra óptica disponibles en el mercado. Por otro lado, la latencia (el tiempo de respuesta de la red) también experimenta una mejora significativa. Según los operadores, esta latencia puede reducirse a tan solo 1 milisegundos, un tiempo prácticamente imperceptible para el usuario, lo que permitiría conexiones virtuales en tiempo real sin retrasos apreciables (Flores Erazo, 2022).

**Figura 10**

Redes móviles quinta generación


*Fuente: (Race, 2018)*

A finales de 2018, comenzó a surgir la tecnología conocida como 5G NR (Nueva Radio), marcando sus primeras apariciones en el mercado. El objetivo principal de esta tecnología es la creación de un vasto ecosistema de Internet de las Cosas (IoT) que pueda satisfacer las necesidades de millones de dispositivos conectados, a continuación, algunas características de esta tecnología.

- Año: 2015
- Velocidad: 1 a 10 Gbps.

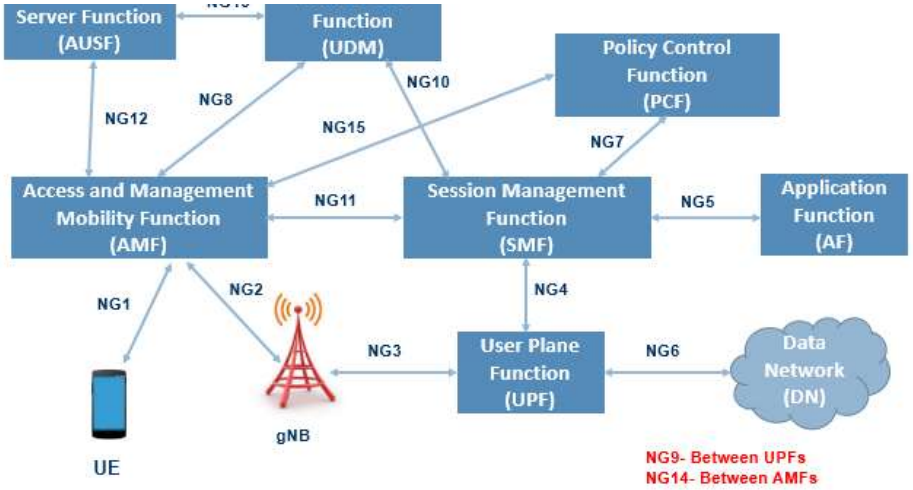
- Ancho de Banda: 1.000 x ancho de banda por unidad de superficie.
- Frecuencia: 3 a 300 GHz
- Tecnologías de multiplexación / Acceso: CDMA y BDMA
- Estándares: banda ancha IP LAN / W AN / PAN & WWWW
- Rendimiento de tiempo real: respuesta rápida, de baja fluctuación, latencia y retardo
- Muy alta velocidad de banda ancha: velocidades de datos Gigabit, cobertura de alta calidad, multi espectro.
- Infraestructura virtualizada: Software de red definido, sistema de costes escalable y bajo.
- Soporta Internet de las Cosas y M2M: 100 veces más dispositivos conectados, Cobertura en interiores y eficiencia de señalización. Reducción de alrededor del 90% en el consumo de energía a la red. Su tecnología de radio facilitará una versión diferente de las tecnologías de radio para compartir el mismo espectro de manera eficiente.
- Servicios: Personas y dispositivos conectados en cualquier lugar en cualquier momento. Su aplicación hará que el mundo real sea una zona Wi Fi. Dirección IP para móviles asignada de acuerdo con la red conectada y la posición geográfica (Arcotel, 2020).

### *4.9.1. Arquitectura quinta generación 5G*

Las redes 5G tienen como características una gran velocidad asociada a latencias de menos de 1 milisegundo, lo que permiten conectividad en tiempo real. La arquitectura de 5G está compuesta por la Radio Access Network (RAN) y los elementos que se encargan de la autenticación que está compuesta por el Next Generation NodeB (gNB) y el Access and Mobility, Management Function (AMF). El gNB hace referencia a la estación base 5G y proporciona servicios de plano de control de usuario NR y plano de control hacia el UE, mientras que el AMF es la función principal e control dentro de la red que interactúa con la RAN y los equipos de usuario (UE) mediante la señalización encriptada a través de las interfaces N2 y N1 respectivamente (Fernández, 2022)

**Figura 11**

Arquitectura quinta generación




*Fuente: (Techplayon, 2020)*

A continuación, se describe cada uno:

- UE: Equipo de usuario
- gNB: Estación base de nodo de próxima generación
- AMF: Función de gestión de movilidad y acceso central
- UPF: Función del plano de usuario
- SMF: Función de control de gestión de sesión
- DN: Red de datos
- AUSF: Función de servidor de autenticación
- UDM: Gestión de datos modificada
- PCF: Función del control de políticas
- AF: Función de aplicación
- NG: Interfaz de red

La autenticación se produce en el AUSF a través del AMF, empleando el Extensible Authentication Protocol (EAP). La red central es el núcleo de las redes 5G, proporciona conectividad segura y confiable a internet y acceso a todos los servicios de la red.

## 4.10. Evolución de la tecnología móvil en Ecuador

**Figura 12**
Redes móviles en el Ecuador

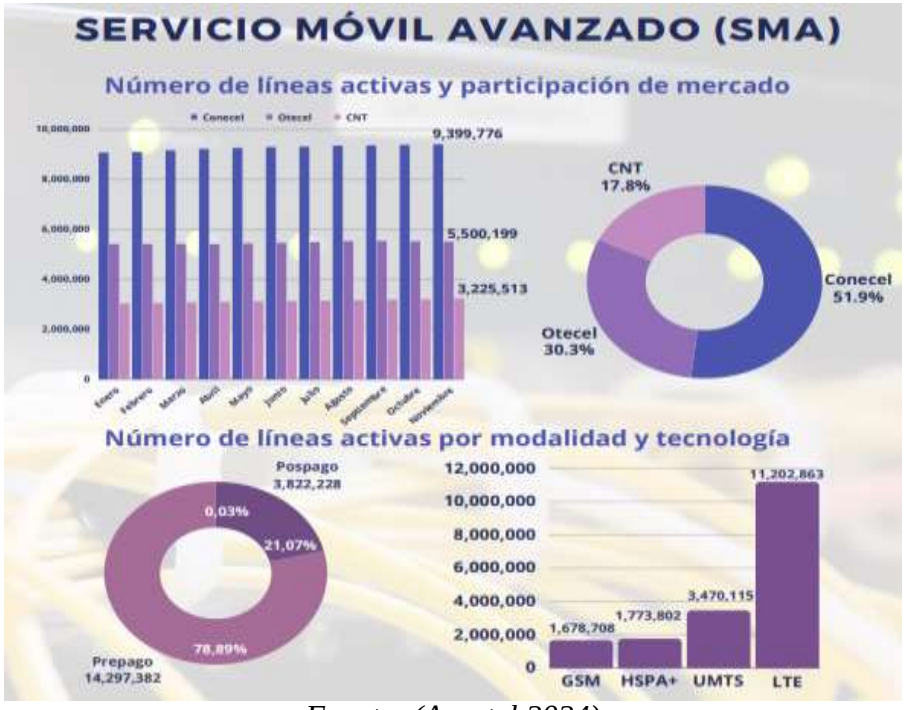

*Fuente: (Redacción, 2023)*

Las tecnologías y servicios móviles de vanguardia se conocen como Servicio Móvil Avanzado (SMA). Estas soluciones de última generación posibilitan una conectividad más ágil y óptima en las redes móviles. Su implementación trae consigo numerosos beneficios, entre los que destacan una mayor rapidez en la transferencia de datos, un considerable mejoramiento en la calidad de las comunicaciones de voz y vídeo, además de incrementar sustancialmente la capacidad y el aprovechamiento de los recursos de red.

De acuerdo al boletín estadístico del mes de enero del año 2023 presentado por la Agencia de Regulación y control (ARCOTEL) y el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) con respecto al servicio móvil avanzado en Ecuador hay una cobertura poblacional de la tecnología 4G del 77,63% y del 95,91% con tecnologías 2G y 3G. La penetración del SMA se define como el total de líneas activas sobre el total de la población a nivel nacional. En los últimos años, desde el mes de enero a noviembre de 2023, el país tenía 18.3 millones de líneas móviles en servicio, de las cuales el 78,89% es prepago y solo un 22% es pospago, esto según estadísticas del ente regulador Arcotel ya que la penetración del internet móvil en ecuador es del 59.4%.

**Figura 13**

Estadísticas del servicio móvil avanzado en Ecuador



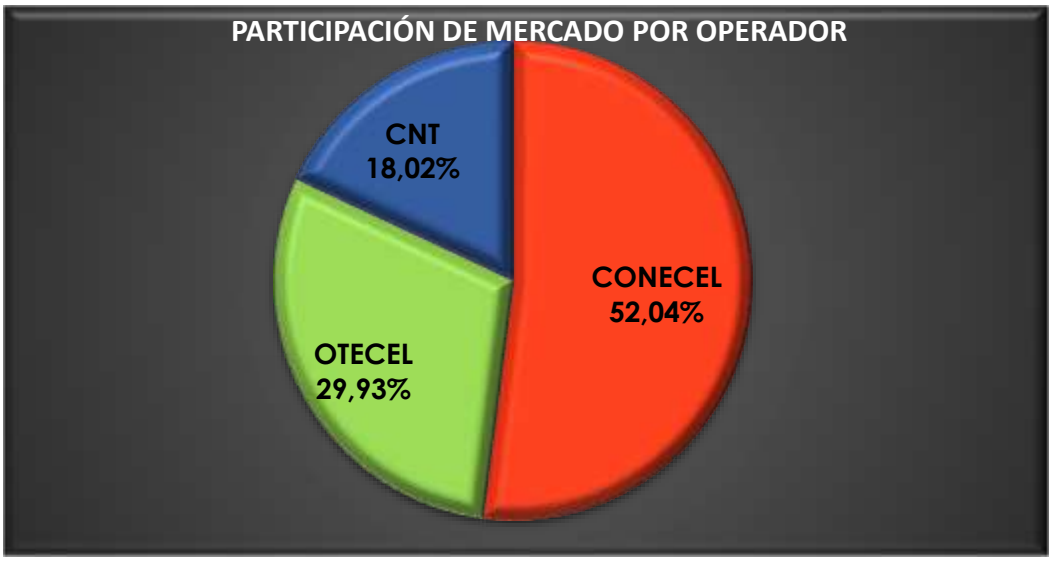

*Fuente: (Arcotel,2024)*

En la actualidad, el Servicio Móvil Avanzado en Ecuador es brindado por tres operadoras principales: CONECEL S.A., OTECEL S.A. y CNT EP. Las dos primeras pertenecen al sector privado, mientras que la última es una empresa pública. Según el Reglamento para la prestación de servicios de telecomunicaciones y servicios de radiodifusión por suscripción, las operadoras privadas requieren de un título habilitante, en este caso, un contrato de concesión para poder ofrecer este servicio de forma legítima, mientras que CNT E.P al ser una empresa estatal, posee la facultad de prestar servicios de telecomunicaciones sin necesidad de título habilitante.

En el mes de febrero del 2024 según reportes estadísticos de Arcotel en la Fig. 8 se puede apreciar una participación de mercado del 52.04% para CONECEL S.A., 29.93% para OTECELS.A. y 18.02% para CNT EP dando un total de 18.129.629 millones de líneas activas a nivel nacional (Arcotel,2024, s. f.).

**Figura 14**

Participación del servicio móvil avanzado por operador




*Fuente: (Arcotel,2024)*

De acuerdo a las estadísticas se puede evidenciar un gran crecimiento de usuarios de SMA, esto sin mencionar las futuras conexiones con máquinas para poder realizar trabajos autónomos. Para todas las operadoras ha existido un crecimiento exponencial y es por ello que deben invertir en infraestructura para la implementación de tecnologías más avanzadas como 5G.

### *4.10.1. Operadora móvil virtual (OMV)*

Este tipo de operadoras son llamadas virtuales, debido a que no poseen licencia para el manejo del espectro radioeléctrico, ya que arrienda y usa este recurso concesionado a otro operador conocido como operador de red que maneja una arquitectura de red móvil completa manejando una menor inversión para ingresar en un mercado determinado.

En ecuador la marca Tuenti que pertenece al grupo Telefónica (Movistar) llegó en el año 2015 con la finalidad de prestar sus servicios de manera virtual, pero a la vez soportado en su infraestructura. De acuerdo a (Redacción, 2023) entre Movistar y Tuenti hay actualmente 5.4 millones de clientes, es decir el 31% del mercado.

Esta operadora virtual Tuenti llegó al mercado con varias promociones de navegación, acumulación de megas y tarifas reducidas, enfocados en llegar a personas jóvenes de 15 a 35 años con acceso a redes sociales ilimitadas mediante combos de debían ser activados por diferentes precios (Telégrafo, 2020).

## 4.11. Seguridad en las redes móviles

La arquitectura de las redes móviles que cuentan con sus respectivos protocolos de seguridad, pero no es de asombrarse que aparezcan muchas vulnerabilidades asociadas a cada generación de telefonía móvil que se han ido mitigando con la implementación de algoritmos con la finalidad de ofrecer un ecosistema seguro y confiable para la comunicación móvil.

En la era digital actual, donde se conectan humanos, cosas y máquinas a través de Internet y dispositivos móviles, la seguridad es fundamental. Los teléfonos inteligentes, que han reemplazado sistemas heredados, están expuestos a amenazas similares a las de las computadoras personales. Las motivaciones de los atacantes también han cambiado, pasando de bromistas inmaduros a redes organizadas de cibercrimen y hacktivistas con objetivos políticos y financieros.

La seguridad adecuada debe incluir inteligencia sobre amenazas, visibilidad y protección en tiempo real. Las herramientas para proteger los sistemas de telecomunicaciones han evolucionado desde el control de acceso físico hasta los modernos antivirus y cortafuegos que tienen en cuenta el contexto y las aplicaciones (Gallego, 2021)

### *4.11.1. Seguridad en redes de primera generación 1G*

El sistema móvil de primera generación utilizaba comunicación analógica, es por ello que fue difícil proporcionar seguridad eficiente en 1G. Un ejemplo fue las escuchas ilegales que cualquiera podía escuchar una comunicación privada entre dos usuarios, ya que todo lo que necesitaba era un receptor que funcione en las frecuencias similares, en conclusión, no había ninguna confidencialidad en las comunicaciones móviles de 1G (Rojo, 2021).

**Tabla 1**

Amenazas y seguridades específicas de la primera generación móvil.

| Vulnerabilidad | Amenazas de Seguridad | Riesgo | Seguridad |
|---|---|---|---|
| - Sin confidencialidad en la comunicación.<br>- No poseía mecanismos de identificación o autenticación para identificar de forma única al usuario. | - Escucha de comunicación privada entre dos usuarios.<br>- Clonación de identidad de manera fácil en teléfonos móviles<br>- Venta de teléfonos clonados ilegales. | - Variable<br>- Los cargos de llamadas realizadas se dirigían al propietario original | - No contaba con seguridad en la comunicación. |

*Fuente: Autor*

De acuerdo a la Fig.13 un atacante puede interferir en la comunicación entre la Estación Base y el Móvil del usuario haciendo pasar como un suscriptor legal para realizar llamadas gratuitas, esto mediante el uso de un radio receptor que clona la información de identidad móvil que es el número del móvil del usuario y su número electrónico serial (ESN) utilizando una laptop con software.

**Figura 15**

Ataque de clonación de teléfonos celulares en la red 1G


*Fuente: (Liyanage et al., 2020)*

### *4.11.2. Seguridad en redes de segunda generación 2G*

El sistema móvil de segunda generación se desarrolló con la necesidad de mejorar la capacidad, calidad y la cobertura de transmisión haciendo posible la transmisión digital en las comunicaciones móviles. La tecnología 2G toma en cuenta cuatro aspectos para la seguridad como la autenticación del usuario, el cifrado de datos y señalización, la confidencialidad de la identidad del usuario y el uso del módulo de identidad del suscriptor (SIM) como un módulo de seguridad. La SIM es una tarjeta inteligente desmontable que contiene la información del suscriptor y se utiliza para demostrar la identidad ante el operador móvil. Para proporcionar la confidencialidad en 2G utiliza la identidad del suscriptor móvil internacional (IMSI) que representa el número único para cada abonado en el mundo y contiene la red local del abonado y país al que pertenece. La tarjeta SIM utiliza algoritmos A3 y A8 entre la estación móvil y el operador móvil (Rojo, 2021).

**Tabla 2**

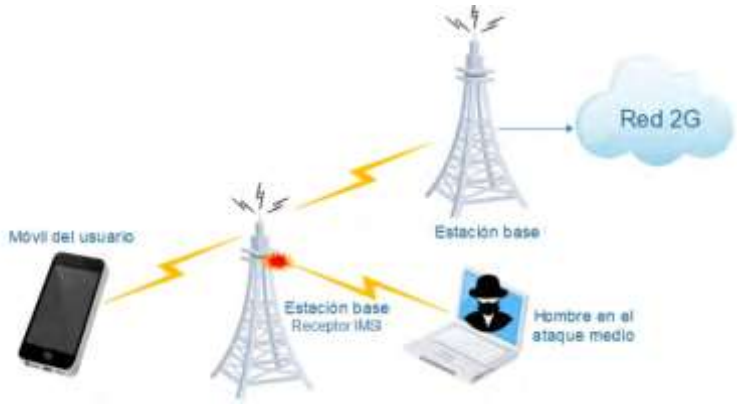
Amenazas y Seguridades específicas de la segunda generación móvil

| Vulnerabilidad | Amenazas de Seguridad | Riesgo | Seguridad |
|---|---|---|---|
| - Mensajes<br>- Creación de estaciones base no autorizado.<br>- Ataques bajo el método ataque intermediario (MitM) | - Spam<br>- Autenticación de red falsa.<br>- Confidencialidad de la identidad del usuario<br>- Denegación de servicio (DoS)<br>- Clonación de identidad IMSI | - Saturación de almacenamiento en el equipo<br>- Información falsa<br>- Interceptación de las comunicaciones móviles | - Protección de cifrado básico para señalización y datos de usuario.<br>- Encriptación de datos y la señal mediante el uso de IMSI, clase de cifrado Ki y algoritmos A3, A8, A5. |

*Fuente: Autor*

Mientras se mitigaba los ataques de la primera generación con la autenticación de usuarios por medio del SIM como un identificador único de usuario, surgió una nueva amenaza llamada hombre en el medio (MitM), que utilizando estaciones base no autorizadas llamados IMSI Catcher los cuales permitían que los usuarios se conecten a canales no seguros, siendo esta otra manera de interferir en la comunicación.

**Figura 16**
Ataque de clonación del IMSI Catcher en 2G




*Fuente: (Liyanage et al., 2020)*

### *4.11.3. Seguridad en redes de tercera generación 3G*

Los sistemas 3G proporcionaron velocidades de datos más altas, mayor capacidad de voz y funciones avanzadas como navegación por internet y el uso de aplicaciones móviles (Rojo, 2021). El estándar UMTS ofreció seguridad en los siguientes segmentos:

- **Acceso a la red:** proporciona al usuario acceso seguro a los servicios 3G brindando protección contra ataques a la interfaz radio.
- **Autenticación de usuario**: es una propiedad de la red que presta el servicio donde confirma la validez de la identidad del usuario.
- **Dominio de Red**: permite que los usuarios puedan cambiar datos de señalización de manera segura y proporciona la protección contra ataques a la red fija.
- **Dominio del usuario:** es el encargado del acceso seguro de las estaciones móvil

**Tabla 3**

Amenazas y Seguridades específicas de la tercera generación móvil.

| Vulnerabilidad | Amenazas de Seguridad | Riesgo | Seguridad |
|---|---|---|---|
| - Aplicaciones de datos e internet<br>- Reemplazo de dispositivos móviles por teléfonos inteligentes<br>- Instalación de aplicaciones no autorizadas. | - Integración de código malicioso en forma de malware y spyware<br>- Sistema operativo<br>- Aplicaciones<br>- Ataques de suplantación de identidad.<br>- Ataques de intermediario.<br>- Ataques de fuerza bruta | - Acceso no autorizado a información personal y confidencial como contraseñas o contactos.<br>- Vulnerable a filtrado de datos, virus, spyware<br>- Degradación de rendimiento de los servicios proporcionados | - Parches y actualizaciones regulares de seguridad<br>- Implementación de políticas de seguridad de aplicaciones estricta<br>- Uso de algoritmos para encriptación de la comunicación. |

*Fuente: Autor*

### *4.11.4. Seguridad en redes de cuarta generación 4G*

El crecimiento del uso del internet dio paso a la banda ancha móvil, ya que los dispositivos móviles integraban aplicaciones relacionadas con la información, la comunicación y el entretenimiento, es por ello que se dio paso al acceso a contenido multimedia de cualquier lugar. Las redes 4G operan completamente con arquitectura y protocolo IP, es por ello que presentan mayores problemas de seguridad en comparación con la generación anterior, por ese motivo, para la autenticación se utilizan credenciales de seguridad, identidad, certificados, nombre de usuario y contraseña (Rojo, 2021).

**Tabla 4**

Amenazas y Seguridades específicas de la cuarta generación móvil.

| Vulnerabilidad | Amenazas de Seguridad | Riesgo | Seguridad |
|---|---|---|---|
| - E-UTRAN<br>- Sistema Operativo inseguro | - Explotación de red de núcleo LTE con identificador temporal<br>- Sistema Operativo inseguro<br>- Descargar aplicaciones no autorizadas<br>- Virus, software malicioso y espía.<br>- DDos (Denegación de servicio distribuido)<br>- | - Obtener acceso a la ubicación del equipo de usuario.<br>- Ataques de interceptación de señalización<br>- Ataques de suplantación de identidad (Spoofing)<br>- Ataques de intermedio (MitM) | - Cifrado de la señal de control de tráfico y los mensajes de comando.<br>- Sistema operativo parchado y actualizado<br>- Instalación de antivirus<br>- Definir una política de acceso al servicio de cada aplicación<br>- Habilitación del cifrado en dispositivos móviles. |

*Fuente: Autor*

### *4.11.5. Seguridad en redes de quinta generación 5G*

El desarrollo de las redes 5G presenta beneficios y riesgos a gran escala. Algunos son similares a las redes cableadas, otros son nuevos; estos se acentúan como en cualquier conexión inalámbrica.

Los usuarios no autorizados pueden acceder al sistema y la información, robar datos, consumir ancho de banda de la red, disminuir el rendimiento de la red o lanzar ataques que impiden que los usuarios autorizados accedan a los servicios o utilizar los recursos para realizar ataques en otras redes. En varias áreas 5G hay muchos riesgos, pero estos se dividen en dos categorías:

- **Ataques pasivos:** Los atacantes intentan obtener o usar la información de los usuarios legítimos, pero no quieren atacar la comunicación. Los ataques pasivos populares en una red celular se clasifican en dos categorías: escuchas clandestinas y análisis de tráfico. Los ataques pasivos tienen como objetivo violar la privacidad y la confidencialidad de los datos del usuario.

- **Ataques activos:** Por otro lado, los ataques activos pueden incluir la alteración de los datos o la interrupción de la comunicación legítima. Los ataques de Hombre en el Medio (MiTM), los ataques de repetición, los ataques de Denegación de Servicio (DoS) y los ataques de Denegación de Servicio Distribuido (DDoS) son ejemplos comunes de ataques activos (Poot, 2022).

Los atacantes cibernéticos continúan explorando nuevas formas de escapar de la detección, habiendo aprendido a explotar el sistema social y financiero para sus necesidades. Con la evolución de los sistemas de pago digitales y la incorporación de tecnologías como Bitcoin a la corriente principal, será mucho más sencillo para los delincuentes permanecer ocultos y seguir obteniendo beneficios financieros.

Según el Proyecto de Asociación de Tercera Generación(3GPP) la transición a redes a 5G se divide en dos partes; 5G No autónomo, que depende de 4G LTE, ya que utiliza sus mismos protocolos del Plano de Control y 5G Autónomo, donde se introduce una Red de Núcleo 5G de manera individual sin depender de LTE.

### *4.11.6. Riesgos de 5G No Autónomo*

Se caracteriza por usar los protocolos del plano de control LTE y adquiere los mismos riesgos heredados de 4G, esto simplemente por tener los mismos componentes y utilizarse de manera inalámbrica. En la Tabla se describen las amenazas principales.

**Tabla 5**
Amenazas y Seguridades específicas de 5G No Autónomo

| Amenazas de Seguridad | Riesgo | Seguridad |
|---|---|---|
| - Ataque de degradación | - Obliga a una conexión de usuario LTE al conectarse a 2G o 3G | - Conexiones cifradas |
| - Ataque de modificación de datos | - Se puede realizar la modificación de datos mediante la técnica hombre en el intermedio (MitM) | - Corroborar con el receptor si la información enviada es la correcta. |

| | | |
|---|---|---|
| - Seguimiento del IMSI | - Cuando se envía solicitudes al IMSI sin cifrar por la Radio, permite al atacante averiguar la información de la SIM | - Autenticación |
| - Roaming LTE | - Uso de protocolos de señalización antiguos con vulnerabilidades permiten rastreo de mensajes y escuchas de conversaciones de voz | |

*Fuente: Autor*

### *4.11.7. Riesgo de 5G Autónomo*

El 5G autónomo ya no depende de 4G, por lo tanto, sus riegos son independientes de 4G. La principal diferencia es que en 5G hay una mejora en la privacidad ya que utiliza una arquitectura basada en servicios con técnicas como Radio definido por Software (SDN) y la Virtualización de Funciones de Red (NFV) que a su vez exponen debilidades en 5G. Algunas vulnerabilidades se deben a la arquitectura que utiliza, una autenticación débil, falta de cifrado o simplemente inseguridad en dispositivos finales (Poot, 2022).

**Tabla 6**

Amenazas y Seguridades específicas de 5G Autónomo

| **Amenazas de Seguridad** | **Riesgo** | **Seguridad** |
|---|---|---|
| - Secuestro de datos | - Los malwares especializados explotan, cifran y bloquean el acceso a datos críticos permiten el acceso mediante pagos por rescate | - Conexiones cifradas |
| - Malware avanzados | - Dirigido a miles de millones de dispositivos móviles y de IoT con capacidad para explorar las vulnerabilidades del sistema operativo y de la red. | - Seguridad de autenticación |
| - Botnets de IoT | - Son dispositivos móviles que alojan un agente/bot de control que recibe comandos remotos y filtra información de un bot maestro. | - Identificación de dispositivos |
| - Fraude, escaneo de puertos IP | - El uso de aplicaciones se puede dar para ataques de escaneo de puertos con la finalidad de robar la información | - Protección física y lógica. |

*Fuente: Autor*

El uso de sistemas operativos móvil los cuales publican parches y actualizaciones con la finalidad de cerrar vulnerabilidades conocidas que puedan comprometer el dispositivo o violaciones importantes de seguridad, ya que los atacantes buscan oportunidades para aprovechar estas vulnerabilidades y obtener acceso no autorizado a dispositivos móviles. Es fundamental que todos los operadores móviles posean conocimiento completo de cómo funciona sus operadores de red en tiempo real con el objetivo de ofrecer una mejor garantía del servicio y más aún proteger su infraestructura de amenazas críticas a su seguridad (Poot, 2022).

## 5. Metodología

El presente trabajo de titulación se basará en una metodología mixta descriptiva, cuyo objetivo es comprender y proporcionar descripciones detalladas sobre la seguridad de las redes 4G y 5G. En el contexto de este proyecto, esta metodología es adecuada para analizar y describir el análisis de las redes móviles en cuanto a sus vulnerabilidades y que mejoras proponer en el campo de la seguridad.

Para desarrollar este trabajo, se efectuará una investigación minuciosa de trabajos como; papers, tesis, publicaciones científicas, en específico artículos académicos, informes técnicos, normativas y estándares de seguridad, entre otros recursos disponibles en línea. Se evaluará cada uno de ellos y se realizarán comparaciones sobre la seguridad de las dos redes móviles con la finalidad de determinar sus vulnerabilidades y la seguridad que se emplea en casos específicos.

**Etapa I: Redes móviles 4G y 5G.** Se especifica las definiciones de estas tecnologías móviles como sus características y su arquitectura de las redes 4G y 5G.

**Etapa II: Análisis de principales amenazas, revisión de casos de estudio y comparativa de estas amenazas en redes móviles 4G y 5G.** Se detallan las principales amenazas que afectan a estas redes móviles, se revisan casos de estudio y se realiza una comparativa en las redes móviles 4G y 5G.

**Etapa III: Evaluación de nuevas tecnologías para la seguridad en redes 5G.** Se especifican las nuevas tecnologías de radio definido por software (SDN) y la virtualización de red (NFV)

**Etapa IV: Recomendaciones y medidas de seguridad en las redes 5G.** Se detallan las principales recomendaciones referente a la seguridad en las redes móviles 4G y 5G que se deben considerar para mantener una buena seguridad al conectarse a estas redes móviles.

**Etapa V: Conclusiones.** Se especifican las conclusiones generales sobre las principales amenazas y las posibles mitigaciones, como el uso de nuevas tecnologías que vuelven a las redes móviles más seguras.

## 5.1 Etapa I: Redes móviles 4G y 5G

### *5.1.1 Redes Moviles 4G*

El desarrollo en la evolución de las redes móviles es la cuarta generación (4G), concretamente LTE. Esta tecnología se está implantando gradualmente en todo el mundo y está ganando impulso, ya que es el estándar elegido por la mayoría de los operadores de telefonía móvil para que los usuarios pasen de las actuales redes CDMA EVDO y 3G HSPA a una experiencia de Internet móvil más rápida.

Según 4G américas, organización que promueve y defiende la implantación de la tecnología 3GPP en datos móviles de banda ancha en todo el continente americano, incluyendo redes, servicios, aplicaciones y dispositivos conectados de forma inalámbrica, LTE tiene capacidad para proporcionar velocidades de descarga de hasta 100 Mbps y de subida de 50 Mbps. Esta tecnología se basa en el protocolo de Internet (IP) y también puede complementarse con WiFi y Femtoceldas para garantizar una cobertura completa (Analuisa, 2014).

En la actualidad, los importantes avances de las tecnologías inalámbricas persiguen la eficiencia de las redes, la reducción de costes y la mejora de la calidad del servicio. Por eso, LTE ofrece varias mejoras en comparación con otras tecnologías, como velocidad de transmisión, eficiencia del espectro, baja latencia, etc. Como resultado, se puede introducir una amplia gama de nuevos servicios, incluido el streaming de vídeo.

### *5.1.2 Definición de la tecnología móvil 4G*

La tecnología 4G se soporta en el estándar 3GPP que se basa totalmente en el protocolo IP, funcionando como un sistema y una red que se consigue mediante la convergencia de las redes por cable e inalámbricas. Esta tecnología puede ser utilizada por módems inalámbricos, teléfonos inteligentes y otros dispositivos móviles. La principal diferencia con las generaciones anteriores será la capacidad de proporcionar velocidades de acceso superiores a 100 Mbit/s en movimiento y 1 Gbit/s en reposo, pero lo más importante es que mantenga calidad de servicio (QoS) con una seguridad de extremo a extremo de alta calidad que permita la prestación de servicios de cualquier tipo en cualquier momento y lugar, al menor coste posible (Ortega, 2010).

### *5.1.3 Características de la tecnología 4G*

El nombre del sistema que da soporte al 4G se denomina en términos más técnicos Long Term Evolution (LTE) y presenta una serie de cambios de configuraciones y características frente a la tecnología anterior. Entre sus requisitos encontramos una velocidad de 100 Mbps en el enlace descendente y 50 Mbps en el enlace ascendente. Además, se trabaja con un ancho de banda que varía de 1 MHz a 20 MHz, la latencia debe ser inferior a 5 ms y respecto a la cobertura debe ofrecer prestaciones máximas en un rango de 5 km y posibilidad de alcanzar rangos de 100 km (García, 2019).

A continuación, se describen algunas características de la tecnología 4G:

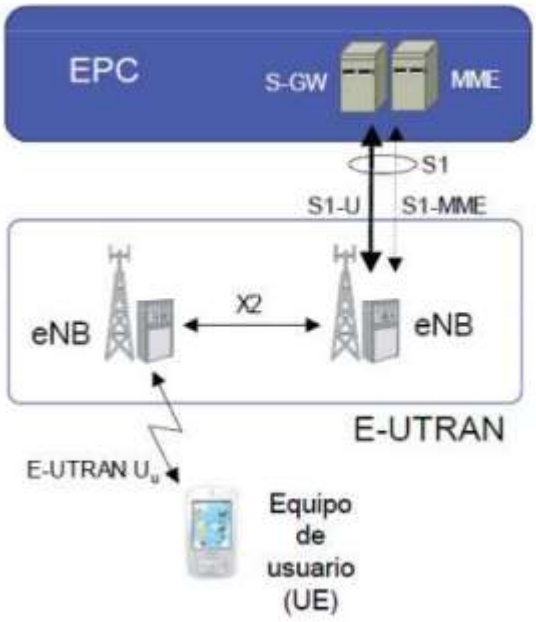
- Alta eficiencia espectral
- Muy baja latencia con valores de 100 ms para Control-Plane y 10 ms para el User-Plane
- Ancho de banda adaptativo: 1,4,3,5,10,15 y 20 MHz
- Compatibilidad con otras tecnologías de 3GPP
- Red de frecuencia única OFDM
- Bajada: 326,5 Mbps para 4x4 antenas, 172,8 Mbps para 2x2 antenas
- Subida: 86,5 Mbps
- Mas de 200 usuarios por celda, celda de 5MHz
- OFDM de enlace descendente robusto frente a las múltiples interferencias y de alta afinidad a las técnicas avanzadas como la programación de domino frecuencial del canal dependiente y MIMO

Esta tecnología transformara las conexiones actuales, ya que los usuarios podrán acceder a la transmisión de contenidos y de datos de manera continua, a una velocidad 10 veces mayor en comparación con la tecnología 3G, con usuarios que podrán navegar fácilmente con mayor estabilidad y calidad de servicio (Gutierrez, 2021).

### *5.1.4 Arquitectura de la red móvil 4G*

El 3GPP ha especificado en su Release 8 los componentes y requisitos de la arquitectura EPS, que servirá de base para las redes de próxima generación. Las especificaciones abarcan dos áreas clave de atención, a saber, LTE y SAE, que han dado lugar a las siguientes especificaciones:

**Figura 17**
Arquitectura red móvil 4G




*Fuente: (Oviedo, 2022)*

A continuación, se describen cada elemento que conforma la arquitectura de 4G:

- Equipo de usuario (UE): Dispositivo movil que permite a los usuarios conectarse a la red LTE y disfrutar de los servicios proporcionados a través de una interfaz radio.
- Evolución UTRAN(E-UTRAN): El elemento importante de la arquitectura E-UTRAN es el nodo B (conocido como eNodo B o eNB). Este proporciona una interfaz con terminales de plano de control de protocolo hacia la UE y el plano de usuario.
- Núcleo de Paquetes Evolucionado (EPC): La entidad de control de la movilidad (MME) es la encargada del plano de control y el Serving Gateway(S-GW) es el responsable del plano de usuario, más un nodo de enrutamiento a redes externas llamado Packet Data Network Gateway (PDN-GW) (Oviedo, 2022).

### *5.1.5 Redes Móviles 5G*

A medida que ha avanzado la tecnología móvil desde la primera hasta la quinta generación, se han producido enormes progresos y transformaciones en cortos períodos de tiempo. Sin embargo, el rápido incremento de usuarios que se conectan diariamente mediante sus dispositivos móviles, así como la diversificación de los tipos de tráfico y uso de datos en estas redes, está generando limitaciones de rendimiento y nuevos desafíos por resolver. La creciente demanda y las cambiantes necesidades sobre las redes están ahora causando cuellos de botella en el rendimiento y nuevos desafíos por abordar.

**Figura 18**
Redes móviles 5G


*Fuente: (Joseph, 2022)*

El despliegue del 5G pretende alcanzar un mundo plenamente inalámbrico en el que no haya falta de cobertura, bajas en el rendimiento ni cortes en las llamadas, es por ello se le ha otorgado la denominación World Wide Wireless Web (WWW).

La tecnología 5G introducirá una serie de mejoras que transformarán muchos aspectos de nuestra vida cotidiana. La más evidente será un incremento sustancial en la velocidad de descarga de datos, posibilitando una transmisión prácticamente instantánea de todo tipo de contenidos sin importar su tamaño. Esto además potenciará servicios ya existentes con 4G como streaming, multimedia, monitoreo de dispositivos, etc. Otro efecto será la aparición de equipos más compactos, eficientes, rápidos y económicos, con aplicaciones en IoT. También se reducirá drásticamente la latencia, pasando de 5ms en 4G a menos de 1ms con 5G, facilitando tecnologías como vehículos autónomos y avances en automatización industrial. Se utilizarán frecuencias de

transmisión mucho más altas dentro del espectro, brindando un ancho de banda extremadamente amplio con múltiples capacidades, pero con la desventaja de que estas ondas de alto rango tienen un alcance limitado y son bloqueadas por objetos. Esto obliga a implementar una gran cantidad de repetidores para expandir la cobertura a zonas extensas (Lopa M & Vora, 2015).

La tecnología 5G representa la generación más reciente en cuanto a redes de comunicación móviles. Esta se perfila como un progreso importante frente a las especificaciones 4G previas. Las redes 5G brindan conectividad con mayor velocidad de transferencia de datos, menores tiempos de respuesta (latencia) en la comunicación, así como soporte para la vinculación simultánea de una mayor cantidad de dispositivos, en contraste con las capacidades de las redes 4G precedentes. En términos generales, la tecnología 5G constituye un avance destacado en el campo de las telecomunicaciones móviles

Si bien la tecnología 5G trae consigo velocidades más rápidas y capacidades avanzadas de conectividad entre dispositivos, su adopción implica a su vez nuevos retos en materia de ciberseguridad que deberán enfrentarse. Dado que representa una red de altísimas prestaciones, su implementación la vuelve más susceptible a ciberataques sofisticados. Los actores maliciosos pueden sacar ventaja de vulnerabilidades en el despliegue de 5G para acceder a información confidencial de los usuarios, interrumpir u obstaculizar la calidad de su servicio e incluso sabotear infraestructura tecnológica crítica. Se deberán mejorar medidas preventivas de monitoreo, detección temprana y respuesta a incidentes para proteger a clientes y operadores de posibles riesgos emergentes asociados al potencial intrínseco de esta innovadora generación de telefonía móvil (Castillo et al., 2022).

### *5.1.6 Definición de la tecnología móvil 5G*

5G es la quinta generación de redes de comunicaciones móviles basada y cimentada en la red 4G LTE. Permite realizar varios servicios de forma más rápida y eficaz con una velocidad de transferencia de 10 Gbps aproximadamente, lo. que permite reducir la latencia y mejorar la flexibilidad de los servicios inalámbricos, mucho mayor que la red móvil 4G LTE. Además, cuenta con una gran estabilidad de conexión e interacciones con el IoT.

Frente a esto, no es un secreto que los usuarios entre mejor servicio tienen, quieren más velocidad y menos tiempo de espera. Por eso llega la 5G, la nueva generación de redes inalámbricas, capaz de soportar 1000 veces más el tráfico que la red actual de 4G y será diez (10) veces más rápido que la red 4G LTE. 5G será la base esencial para proyectos de realidad virtual, conducción autónoma, IoT, automatización de sistemas y mucho más (Fuentes & Ibáñez, 2019).

### *5.1.7 Características de la tecnología 5G*

La tecnología 5G está definida por nueve especificaciones que mejoran significativamente la comunicación. Entre estas especificaciones está la latencia, que se refiere al tiempo que tarda la información en viajar desde su origen hasta su destino. Con una latencia de sólo un milisegundo, la tecnología 5G garantiza una notable mejora de la comunicación.

A continuación, se describen algunas características de la tecnología 5G:

- 100% de cobertura para lo cual será necesario realizar millonarias inversiones a nivel de infraestructura física.
- Contará con un ancho de banda de 1.000 por unidad de área.
- Un dispositivo IoT (Internet de las cosas) contará con una vida útil de 10 años de baja potencia.
- Contará con velocidades, dependiendo el dispositivo, hasta de 10 GB por segundo.
- Reducirá el consumo de energía en la red hasta en un 90%.
- Aumentará el número de dispositivos conectados de 10 a 100x lo cual se calcula en un promedio de 50.000 millones de dispositivos conectados de forma simultánea.
- Frecuencia de 3 a 300 GHz
- Se tendrá un 99.99% de disponibilidad de la red.
- Las redes 5G usaran los estándares de seguridad SE, HSM, OTA y KMS con el fin de que la información enviada no sea atacada (Castillo et al., 2022)

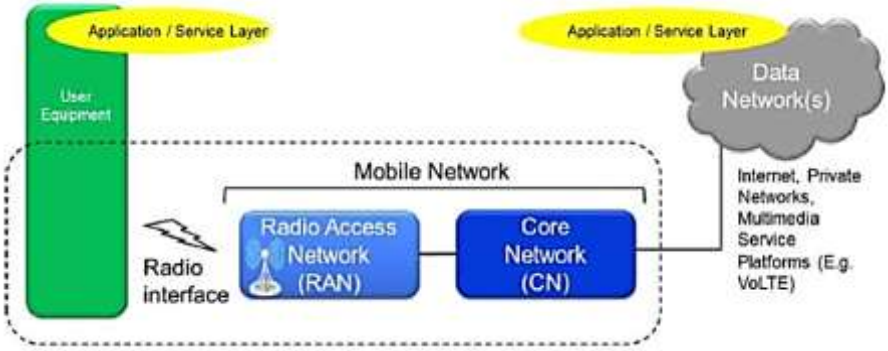
En lo que respecta a las características, no hay duda de que el 5G revolucionara la forma en que navegamos y utilizamos Internet hoy en día, todo gracias al notable crecimiento de los servicios móviles. Un aspecto crucial de las redes 5G es su capacidad para proporcionar acceso a

todos los dispositivos dentro del rango de conexión, y lo mejor es que los canales no se sobrecarguen, ni experimentaremos frecuentes caídas de señal o errores.

### *5.1.8 Arquitectura de la tecnología móvil 5G*

Las especificaciones de la red central 5G fueron desarrolladas por el 3GPP en la versión 15, entre 2018 y 2019. Estas especificaciones diseñan principalmente la arquitectura de la red central en los dos escenarios de red 5G definidos (Stand-Alone y Non-Stand-Alone) también definidos en la versión 15. Al igual que los sistemas anteriores, como LTE, la arquitectura del sistema 5G abarca tres grandes bloques (Fernández, 2022)

**Figura 19**
Bloques principales del sistema 5G




*Fuente: (Fernández, 2022)*

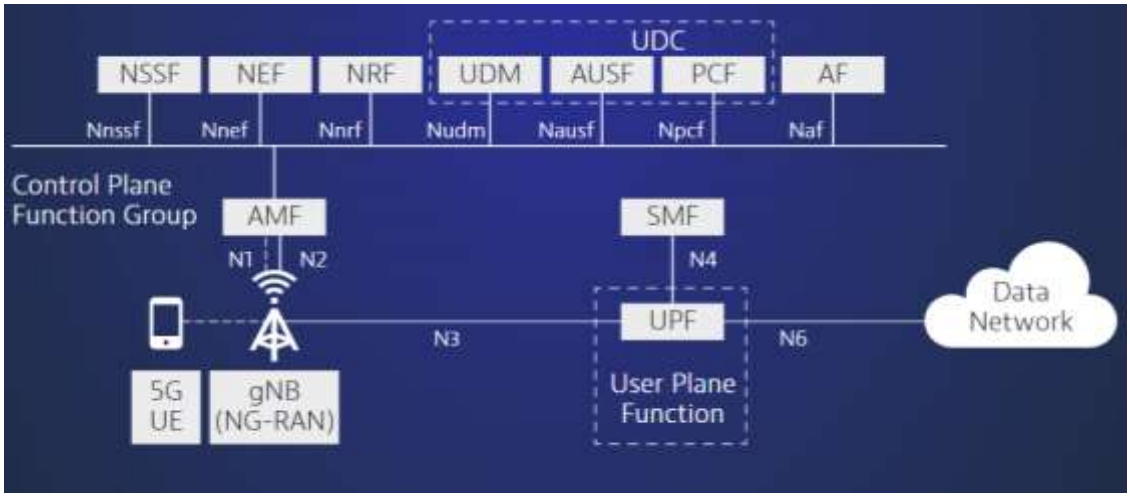
A continuación, se describen algunas características de la tecnología 5G:

- User Equipment (UE): Equipo de usuario
- 5G Core Network (5GC): responsable de las funciones no relacionadas con el acceso por radio, tales como autenticación, carga, configuración de conexiones de extremo a extremo y gestión de movilidad.
- Next Generation- Radio Access Network (NG-RAN): responsable de toda la funcionalidad del sistema relacionado con la radio.

La arquitectura de las redes centrales 5G constituye la base de las nuevas especificaciones de la tecnología 5G, garantizando el aumento de capacidad que exige esta tecnología. La nueva red central 5G, definida por el 3GPP, utiliza una arquitectura basada en servicios (SBA) alineada con la nube, que abarca todas las interacciones y funciones de la tecnología 5G, incluida la autenticación, la seguridad, la gestión de sesiones y la incorporación del tráfico de los dispositivos finales. La red central 5G mejora aún más la NFV con funciones de software virtualizadas implementadas a través de la infraestructura MEC, que es esencial para los principios de la arquitectura de la tecnología 5G (Viavi, 2023).

**Figura 20**

Arquitectura del núcleo de la red 5G




*Fuente: (Viavi, 2023)*

A continuación, se describirá cada uno de los componentes cables de una red central 5G:

- Los equipos de usuario (UE), los dispositivos celulares 5G, se conectan a través de la nueva red de acceso radioeléctrico 5G al núcleo 5G y, además, a las redes de datos (DN), como Internet.
- La función de gestión del acceso y la movilidad (AMF) actúa como punto de entrada único para la conexión del equipo de usuario.
- Basándose en el servicio solicitado por el UE, la AMF selecciona la respectiva función de gestión de sesión (SMF) para gestionar la sesión de usuario.
- La función de plano de usuario (UPF) transporta el tráfico de datos IP (plano de usuario) entre el equipo de usuario (UE) y las redes externas.

- La función de servidor de autenticación (AUSF) permite a la AMF autenticar al UE y acceder a los servicios del núcleo 5G.
- Otras funciones como la función de gestión de sesiones (SMF), la función de control de políticas (PCF), la función de aplicación (AF) y la función de gestión unificada de datos (UDM) proporcionan el marco de control de políticas, aplicando las decisiones de política y accediendo a la información de suscripción, para gobernar el comportamiento de la red.

La arquitectura de la red 5G es más compleja, pero esta complejidad es necesaria para ofrecer un mejor servicio que pueda adaptarse a las necesidades de las diferentes aplicaciones que hoy en día se utilizan.

## 5.2 Etapa II: Análisis de Amenazas en la seguridad de redes móviles 4G y 5G

La tecnología 5G está diseñada para ofrecer velocidades máximas de múltiples Gbps, latencias ultra bajas, más confiabilidad, capacidad de red masiva, mayor disponibilidad y una experiencia de usuario más uniforme para más usuarios. Al existir un gran rendimiento y una mayor eficiencia, esto brinda al usuario nuevas experiencias y aporta a que industrias se adapten a estos mecanismos de comunicación.

La seguridad es un factor importante en el funcionamiento de las redes 5G ya que debe poseer de controles de seguridad para garantizar la confidencialidad, integridad, disponibilidad de tal modo que la red pueda ofrecer a los usuarios una plataforma de comunicación segura (Cruz, 2022).

### *5.2.1 Ataques a la disponibilidad*

La disponibilidad se basa en la capacidad de un sistema o servicio para estar en funcionamiento y accesible para los usuarios en todo momento. A continuación, se describen las amenazas a la disponibilidad:

- **Virus**

  Son un tipo de malware que se autorreplican por medio de otro sistema o persona para circular. Una vez infectado un teléfono móvil puede convertirse en una fuente de propagación del virus con el objetivo de enviar mensajes de texto y correos electrónicos a otros dispositivos vulnerables, llevando a otros usuarios a abrir o descargar estos virus. Los virus también pueden venir en forma de malware ocultos en aplicaciones que el usuario descarga sin conocimiento alguno.

- **Gusanos**

  Son casi idénticos a los virus, excepto por una diferencia y es que no requieren asistencia externa, lo que significa que se autorreplican dentro de la red y no requieren la interferencia de un usuario. El gusano Cabir fue el primer gusano creado y es multiplataforma, lo que significa que puede infectar varias plataformas.

- **Botnets**

  Una red de máquinas controlada por un botmaster se conoce como botnet, que se utiliza para realizar ataques maliciosos. Un bot o zombie es una computadora o sistema que está controlado por un botmaster. Este problema puede tener un impacto significativo en el dispositivo y aumenta la probabilidad de que los teléfonos inteligentes se conviertan en bots. Para reconocer si un teléfono móvil se encontraba infectado se debía tener en cuenta lo siguiente:

  - Lentitud en el teléfono móvil, retrasos con más frecuencia y el rendimiento del sistema era sumamente lento.
  - El dispositivo se reiniciaba solo o se quedaba inhibido de vez en cuando.
  - Incluso sin aplicaciones que lo requieran, el dispositivo inteligente enviaba y recibía datos con frecuencia.
  - Comportamiento extraño del sistema.

- **Ataques de denegación de servicio (DDoS)**

  El ataque de denegación de servicio ocurre cuando un atacante intenta hacer que un sistema o dispositivo sea inaccesible inundándolo con datos que obligarán al dispositivo a usar sus recursos, lo que lo hace inaccesible. El atacante se asegura de que los usuarios de ciertos servicios no puedan usarlos en este caso, las redes inalámbricas suelen ser más vulnerables a este tipo de ataques. Por general el acatante

inunda el punto de acceso o el servidor de comunicación con una gran cantidad de solicitudes, lo que mantiene ocupado al servidor tratando de responder a estas solicitudes en lugar de conectarse con lo que el usuario real desea.

- **Ransomware**

  El malware de rescate, también conocido como ransomware, es un tipo de malware que impide a los usuarios acceder a sus archivos personales y exige que paguen un rescate para poder acceder a ellos de nuevo. Los primeros tipos de ransomware se desarrollaron al final de la década de los 80, y el pago debía hacerse por correo postal. Los creadores de ransomware exigen hoy que se pague con criptomonedas o tarjetas de crédito (Garcia, 2020).

### *5.2.2 Ataques a la confidencialidad*

La confidencialidad es el acceso a la información trasmitida entre el emisor y receptor o varios destinatarios que estén autorizados. La violación a la confidencialidad se da cuando un atacante tiene acceso a la información de un dispositivo móvil. A continuación, se describen las amenazas a la confidencialidad:

- **Malware**

  El malware, también conocido como software malicioso, es una pieza de software que se utiliza para atacar el sistema operativo de una víctima para realizar una serie de operaciones dañinas, como interrupciones del sistema, eliminación o modificación de datos, recopilación de información y datos confidenciales, obtener acceso no autorizado al sistema o incluso tomar el control del dispositivo. Virus, gusanos, troyanos y spyware son algunos de los muchos tipos.

- **Spyware**

  El spyware es un tipo de virus que rastrea sus actividades y ubicación mientras roba sus datos personales. El spyware a veces se combina con otro software que parece ser legítimo y aprovecha su presencia en segundo plano para recopilar datos de manera discreta. Los Keyloggers son programas de spyware que alojados en el software realizan capturas de pantalla de las ventanas que estamos utilizando.

- **Adware**

  Este malware es el que "bombardea" tu teléfono con ventanas emergentes de anuncios. El código malvertising, que se incrusta en las publicidades dentro de las aplicaciones y aprovecha las vulnerabilidades del sistema operativo para infiltrarse en el móvil y robar datos personales, es otra forma en que se puede presentar.

- **Hombre en el Medio (Man-in-the-Middle)**

  Un ataque Man-in-the-Middle (MitM) es una especie de ataque cibernético en el que un atacante no autorizado entra en una comunicación en línea entre dos usuarios. El malware que se encuentra en medio del ataque monitorea con frecuencia y modifica la información clasificada individual que los dos usuarios acaban de obtener. Aunque MitM se puede proteger con cifrado, los atacantes exitosos redirigirán el tráfico a sitios de phishing diseñados para parecer legítimos o simplemente pasarán el tráfico a su destino previsto una vez que se hayan cosechado o registrado, lo que hace extremadamente difícil detectar tales ataques (Garcia, 2020)

### *5.2.3 Ataques a la integridad*

La integridad de la información se refiere a la calidad de la información que garantiza que sea precisa, completa y fiable a lo largo de su ciclo de vida. La integridad garantiza que la información no ha sido manipulada de manera malintencionada o accidental, y que su contenido es auténtico y no ha sido modificado sin autorización (Calderón, 2023). A continuación, se describen las amenazas a la integridad:

- **Troyanos**

  El término "Troyanos" se refiere a un tipo de software malicioso que se disfraza para ocultar sus verdaderas intenciones. Sin embargo, a diferencia de los virus, no puede infectar ni expandirse por sí solo. Esta categoría de malware se basa en otros medios, como descargas automáticas, explotación de vulnerabilidades, descarga por otro código malicioso o técnicas de ingeniería social, para infiltrarse en el dispositivo de una víctima.

- **Sybil**

  El ataque de Sybil es otro ataque a la integridad de un sistema el cual ataca las redes móviles y daña la integridad de los datos al enviar una gran cantidad de datos falsos. El objetivo principal de este ataque es obtener la mayoría de la influencia en la red para llevar a cabo acciones ilegales en el sistema. Esto puede ser tan simple como crear una cuenta de redes sociales.

## 5.3 Casos de estudio referente a las amenazas en redes móviles 4G Y 5G

En los siguientes casos de estudio se analizan algunos ejemplos de cómo se puede vulnerar las seguridades de las redes móviles 4G Y 5G.

### *5.3.1 Caso de estudio: Seguridad en el plano de control de las redes móviles 5G contra amenazas DoS*

El principal objetivo de este caso de estudio es analizar los problemas de seguridad que enfrenta el plano de control de la red de acceso de radio 5G (5G-RAN) debido a las mejoras funcionales y arquitectónicas realizadas en la capa del protocolo de control de recursos de radio (RRC). Los ataques DoS planteados en generaciones de redes móviles anteriores también se pueden llevar acabo hacia la infraestructura de 5G NG-RAN con la finalidad de sobre cargar el plano de control de señalización, lo que puede alterar el funcionamiento normal de la red y dar lugar a una pérdida de productividad desde la perspectiva del operador de la red móvil.

Los sistemas 5G continúan utilizando el protocolo RRC para asignar y liberar recursos de radio entre la red y los usuarios finales. En 5G se implementó un estado RRC llamando INACTIVO con la finalidad de minimizar la latencia reduciendo los intercambios de señalización desencadenados por la transición al estado RRC llamado CONECTADO a través de varios elementos de infraestructura de 5G ya que este estado contribuye a prolongar la duración de la batería de los dispositivos móviles minimizando la señalización causada por frecuentes transiciones de inactivo a conectado (Ettiane et al., 2021).

#### *5.3.1.1 Metodología utilizada en el caso de estudio*

- Llevar a cabo un análisis de rendimiento de los principales progresos en el protocolo 5G RRC y determinar algunas vulnerabilidades de eficiencia relacionadas en el plano de control.
- En su estudio explican y presentan un ataque de denegación de servicio (DoS) basado en RRC que ponen en peligro la disponibilidad de recursos 5G-RAN.
- Presentan y analizan el impacto de los ataques emergentes que explotan las nuevas mejoras en el protocolo 5G RRC ya que este ataque es heredado de generaciones móviles anteriores donde su función es sobrecargar el plano de control para que usuarios legítimos no puedan acceder a los servicios móviles.

#### *5.3.1.2 Análisis de impacto de amenazas de señalización 5G RRC a la disponibilidad*

- Se analiza el impacto de dos ataques DoS que explotan las nuevas mejoras del protocolo RCC en el sistema 5G. Este ataque consiste en sobrecargas el plano de control de 5G, cabe mencionar que este fallo no es nuevo ya que existía en los primeros dispositivos móviles y aun se puede usar para degradar la seguridad de los sistemas 5G actuales.
- Este ataque de señalización DoS aprovecha el tiempo de espera de inactividad que gestionan las transiciones de estado RRC para producir una fuerte carga de señalización con la finalidad de congestionar el plano de control de la red móvil y conducir a una interrupción global, afectando a la disponibilidad de la red.
- En su estudio (Ettiane et al., 2021) demuestran como un adversario puede infiltrase en el tráfico móvil y controlar una cantidad importante de dispositivos mMTC, con la finalidad de infectar sus sistemas operativos con malware o evitando sus controles de autenticación. Posterior a ello el atacante les ordenara que envíen una ráfaga de paquetes cortos con regularidad e inmediatamente después de la expiración del tiempo de espera inactivo para activar frecuentes transiciones de estado inactivo a conectado y viceversa. Estos mensajes de establecimiento y liberación pueden hacer caer la unidad centralizada que constituye el punto de terminación del plano de control y no exista la disponibilidad para dar conexión a un usuario real.

### *5.3.2 Caso de estudio: Seguridad para redes celulares 4G y 5G: un estudio de los esquemas de autenticación y preservación de la privacidad existentes.*

En esta investigación se presenta un estudio de los esquemas de autenticación y preservación de la privacidad existentes para redes 4G y 5G, posterior a ello describen las amenazas en las redes 4G y 5G que incluyen ataques a la privacidad, integridad, disponibilidad y la autenticación. También proporciona una clasificación de las contramedidas en tres categorías como métodos de criptografía, factores humanos y métodos de detección de intrusiones.

#### *5.3.2.1 Metodología usada en este caso de estudio*

En este caso de estudio se describen los principales ataques contra la disponibilidad en 4G, donde este tipo de amenazas intentan interrumpir el comportamiento continuo de un sistema, y se clasifican en seis ataques en esta categoría.

- Ataque primero en entrar, primero en salir (FIFO): Al reunir los intervalos de tiempo de entrada y salida, un adversario fuerte puede lanzar un ataque FIFO.
- Ataque de redirección: Este ataque es fácilmente posible cuando un adversario obtiene la información correcta de la entidad del usuario aumentando la intensidad de su señal para redirigir o haciéndose pasar por una estación base en las redes celulares 4G.
- Ataque físico: Este ataque se puede dar cuando una persona ingresa sin autorización a una estación base con la finalidad de realizar el ataque conectado mediante su laptop.
- Ataque de skimming: Este ataque se da mediante la captura y transferencia no autorizada de datos de pago a otra fuente cuando se utilizan los dispositivos móviles para realizar compras por internet.
- Ataque de denegación de servicio (DoS): Es un ataque donde un intruso tiene como objetivo que un dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el correcto funcionamiento normal del mismo. Estos ataques por lo general sobrecargan o inundan una maquina con la finalidad de que no pueda procesar el tráfico normal y no esté accesible a los usuarios que deseen acceder (Ferrag et al., 2018)

### *5.3.3 Caso de estudio: Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos.*

El objetivo de este estudio es establecer algunos riesgos y posibles efectos de las redes de telecomunicaciones, y como un atacante con pocos recursos computacionales puede eventualmente atacar el sistema, se muestran algunas vulnerabilidades de seguridad en las redes móviles, los riesgos y la posibilidad de explotación, así como recomendaciones generales para reducir estos riesgos.

#### *5.3.3.1 Metodología utilizada para llevar a cabo el análisis de la seguridad en redes móviles 4G*

- Se realizo una investigación de diferentes vulnerabilidades en estas redes de telecomunicaciones.
- Se elaboro un mapa de riesgos para visualizar los posibles impactos.
- Una prueba técnica que consolida un ataque MitM con una captura de tráfico siendo exitosos dicho ataque.
- Finalmente se describen recomendaciones de seguridad en el caso de que se logren ejecutar ciberataques.

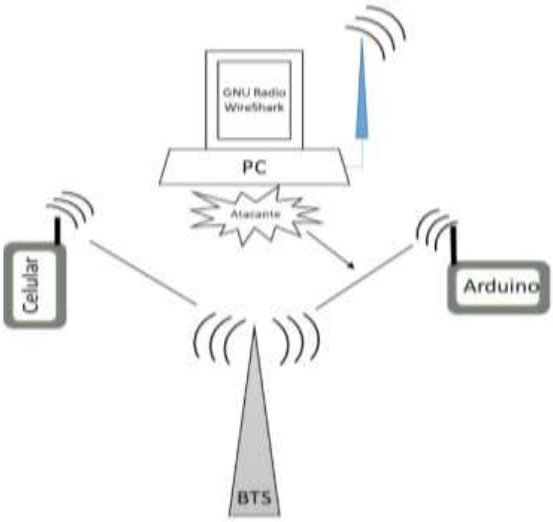
#### *5.3.3.2 Análisis del riesgo de interceptación o robo de información.*

En esta etapa, se realiza una prueba práctica de cómo obtener información del tráfico de red para detectar posibles ataques de tipo MitM, mediante la captura de datos de una llamada móvil en curso. Se analizan parte de los riesgos obtenidos, se configura una arquitectura básica, se utiliza GNU Radio, software para captura de paquetes Wireshark y, finalmente, se ofrecen propuestas para reducir los efectos potenciales (Roldán & Vargas, 2020).

- Para el montaje de la red de prueba (realizando llamadas a través del operador respectivo), se usó un programa desarrollado en Arduino Mega con su modulo GSM-SIM900 para la interceptación de dichas llamadas, se empleó una antena para 3.5G más GNU Radio y se realizaron las respectivas capturas con Wireshark.

**Figura 21**

Diseño del montaje de la interceptación de tráfico




*Fuente: (Roldán & Vargas, 2020)*

- Se considera la conexión del Arduino hacia cualquiera de las antenas BTS disponibles por el proveedor de servicios.

**Figura 22**

Arduino y Modulo Sim900

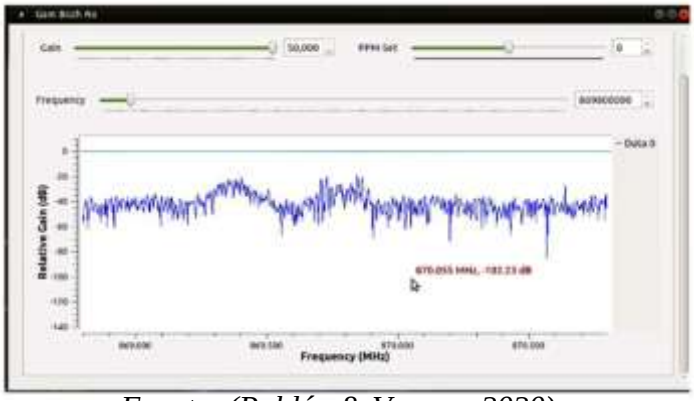
*Fuente: (Roldán & Vargas, 2020)*

- Se conecto la antena 2000 MHz a un Linux con GNU Radio para la escucha del tráfico en tránsito (como antena atacante).
- El tráfico es capturado a través de Wireshark y, con ello, se logró la extracción de la información relevante de las conexiones.
- Se implemento un programa para Arduino con una conexión hacia las redes GSM ya que, una vez compilado el programa, se ejecutó la llamada, la cual es capturada por la antena del atacante.

- Cuando se ejecuta la llamada se tiene activo el programa GNU Radio que localiza un rango de frecuencia entre 870 a 1900 Mhz, frecuencias establecidas por el proveedor móvil, esto con la finalidad de escuchar la transmisión broadcast de todas las posibles llamadas cursantes

**Figura 23**

Ventana de ejecución de GNU Radio

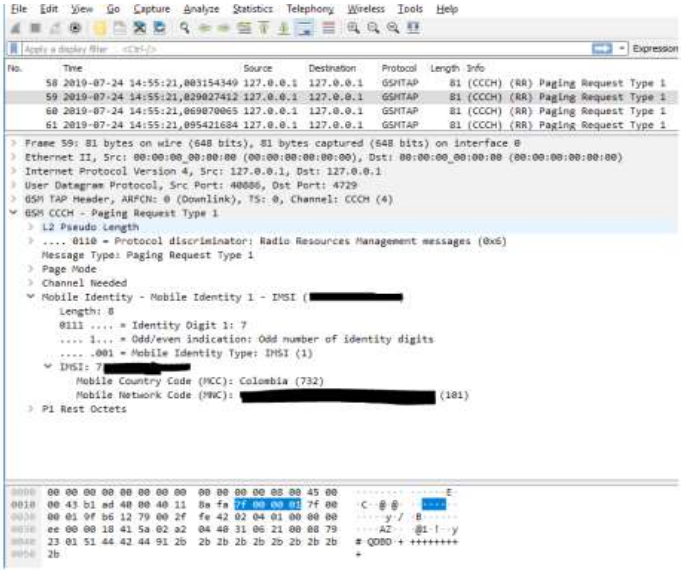



*Fuente: (Roldán & Vargas, 2020)*

- Con la captura de la señal, se activa Wireshark para la visualización de datos cursantes por la antena del atacante.

**Figura 24**

Captura del IMSI con Wireshark




*Fuente: (Roldán & Vargas, 2020)*

- Mediante esta captura simple de información de forma se logró obtener el IMSI y otros datos que con ello se demuestra la posibilidad de que el riesgo de interceptación y robo de información se consolide y sea real
- Finalmente se comprueba que con herramientas básicas un atacante puede obtener información relevante de una llamada telefónica y con ello poder actuar en diferentes frentes de seguridad

#### *5.3.4 Caso de estudio: Ataque a la integridad de usuarios en 5G*

En este estudio se centra en explicar el uso de distintas herramientas utilizadas en el desarrollo del proyecto Open Source (OAI) con la finalidad de crear una red 5G mediante laboratorio usando SDR para la implementación de la red, el uso de una tarjeta SIM y Wireshark para el análisis de trazas entre los diferentes nodos de la red (Gallego, 2021).

##### *5.3.4.1 Metodología utilizada para el caso de estudio*

- Uso de software libre desarrollado por Open Air Interface (OAI), una plataforma de proyectos de redes de acceso radio (RAN) y redes core (CN)
- Se utiliza varios dispositivos SDR, que permiten la configuración mediante software lo que tradicionalmente se ha ejecutado en hardware, obteniendo mejor flexibilidad para el desarrollo de estos proyectos.
- Para el UE se utiliza un dispositivo móvil Oppo Reno 5G, además de una tarjeta SIM.
- Finalmente, para el análisis de las distintas trazas entre la comunicación de los nodos se utilizó Wireshark, herramienta que permite capturar el tráfico de las comunicaciones.

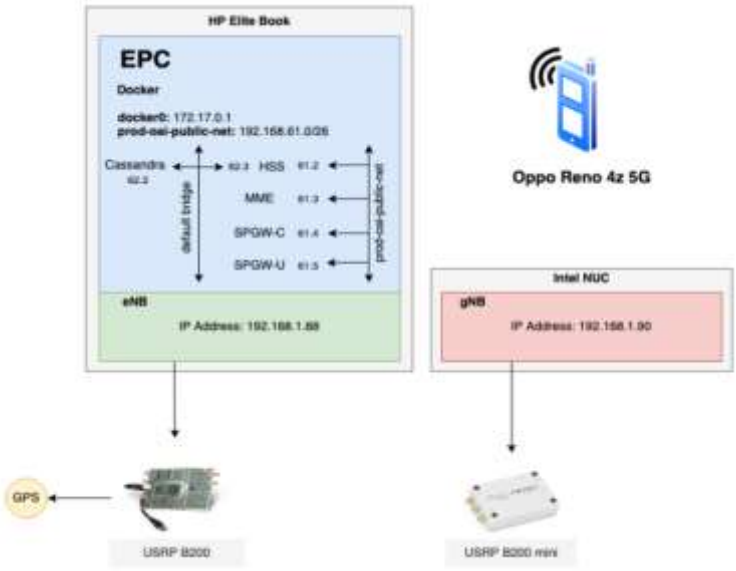
##### *5.3.4.2 Análisis del ataque IMSI Catcher en abonados 5G*

El número IMSI de un usuario es información crucial. Un IMSI Catcher es un ataque que puede interceptar este número mientras se conecta a la red para rastrear la localización del usuario o incluso interceptar tráfico, mensajes de texto o llamadas. Por lo tanto, obtener IMSI es considerado una vulnerabilidad importante dentro de las redes 5G.

La idea principal de este ataque es simular una red móvil o estación base y hacer que el abonado trate de conectarse a esta red, aunque no es necesario que ni se conecte ya que solo se necesitara el IMSI para autenticar al usuario. Esto se podrá lograr con el uso de software SDR y el uso de IMSI Catchers por un valor accesible en el mercado.

**Figura 25**

Arquitectura de 5G-NSA usando USRP

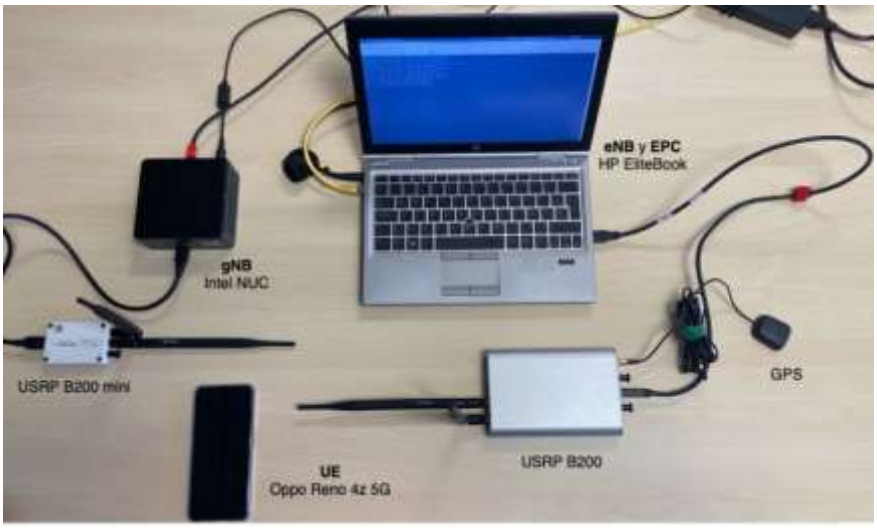



*Fuente: (Gallego, 2021)*

Para que un usuario se intente conectar a la estación base falsa en primer lugar se deberá propagar una señal de radio con más potencia y así el UE intentara conectarse tomando en cuenta que los datos de la operadora móvil coincidan con la tarjeta SIM. Otra manera seria inhibiendo las frecuencias de la tecnología a la que se quiere atacar y así obligar al UE a escanear nuevamente las frecuencias (Gallego, 2021).

**Figura 26**

Escenario de laboratorio




*Fuente: (Gallego, 2021)*

Para dar paso al ataque IMSI Catcher se realizan las configuraciones del EPC en este caso la laptop, los nodos eNB y gNB respectivamente, posterior a ello se comprueba que los nodos se puedan comunicar entre ellos, a continuación, se describe como se obtiene el IMSI.

- Una vez que se ejecutan todos los componentes y nodos de la red 5G se procede a tratar de conectar el UE.
- Cuando el UE trate de conectarse al eNB se recibirá un mensaje en la laptop de (nueva conexión de UE aceptada).
- Este mensaje corresponde con el RRC (Connection Request), ya que es la primera vez que el UE se intenta conectar a esta red, este enviara una identidad aleatoria (random UE identity).
- Una vez que se comprueba si ha llegado este mensaje de intento de conexión, se verifica en los logs del MME el IMSI, puesto que es la primera vez que trata de conectarse a la red, deberá enviar el IMSI en texto claro.
- Con este mensaje ya obtenemos el IMSI del abonado y podríamos perpetrar numerosos ataques, con esto se corrobora la alteración a la integridad de la información del IMSI

**Figura 27**
Obtención del IMSI

```
000536 00049:345289 7F5F188FA700 DEBUG NAS-EM r-
mme/src/nas/emm/emm_data_ctx.c:0197    ue_id=1 set IMSI 901700000013638
(valid)
```

*Fuente: (Gallego, 2021)*

### *5.3.5 Caso de estudio: Ataque a la privacidad de localización celular 4G y 5G*

En este artículo, se demuestra cómo un adversario que se encuentre cerca de una víctima puede aprovechar la naturaleza fija de las ocasiones de búsqueda para conocer la identidad de la víctima (número de teléfono) con su ocasión de búsqueda, con un costo mínimo. El ataque ToRPEDO, que se explica en la investigación utiliza una falla en el protocolo de búsqueda 4G/5G, permite a un atacante que conoce el número de teléfono de una víctima verificar si está presente en un área celular específica e identificar la búsqueda de la víctima. No solo mejora los ataques previos, sino que también facilita los ataques más recientes (Rafiul & Bertino, 2020).

El Ataque Torpedo permite que un adversario pueda verificar la información de una víctima, inyectar mensajes de localización, y montar ataques de denegación de servicio. La metodología utilizada en este caso de estudio es la siguiente:

- Revisión bibliografía respecto al tema de estudio con la finalidad de poder entender los diferentes ataques a la RAN.
- Uso de la identidad del suscriptor móvil temporal aleatoria (TMSI) para dar paso al ataque Torpedo.

#### *5.3.5.1 Demostración del ataque de localización celular 4G y 5G*

El ataque TORPEDO es un ataque que permite localizar, rastrear a usuarios de teléfonos móviles 4G y 5G explotando una vulnerabilidad en el protocolo de paginación. Este protocolo se utiliza para notificar a los dispositivos móviles sobre llamadas o mensajes entrantes cuando estos se encuentran en hibernación. Al enviar mensajes repetidos a un número de teléfono, un atacante puede activar mensajes de búsqueda en la red y así determinar la posición o identidad del dispositivo objetivo.

Mediante este ataque se puede desde rastrear dispositivos móviles, interceptar las comunicaciones o incluso falsificar los mensajes (Rafiul & Bertino, 2020). A continuación, se describen el proceso:

- Cada vez que se cambia el TMSI, una llamada realizada por un atacante y el mensaje de búsqueda resultante ya no se pueden conectar. La sincronización del protocolo de búsqueda entre la estación base y el dispositivo es la idea central de este proyecto de ataque. El protocolo de paginación LTE emplea un ciclo de paginación de tramas T con una duración de 10 ms.
- Mediante el ataque TORPEDO aprovecha la información disponible, incluido el retraso exacto entre el momento en que se realiza la llamada y el momento en que se observa el mensaje de paginación, y el número exacto de registros de asignación en cada cuadro.
- Este ataque calcula la probabilidad de ver las observaciones de los mensajes de localización cuando el PFI del dispositivo de la víctima toma cualquier valor en (1, 1 …T-1) ya que el dispositivo de la víctima está presente.

#### *5.3.5.2 Impacto en la seguridad del ataque TORPEDO*

Este ataque no solo se aplica en 4G sino también en 5G, ya que una vez que el atacante conoce la ocasión de búsqueda de la víctima haciendo uso de Torpedo este puede secuestrar el canal de búsqueda de la víctima. Eso permitirá al atacante montar un ataque de denegación de servicio inyectando mensajes de paginación vacíos y fabricados logrando que la víctima reciba cualquier servicio pendiente por ejemplo un SMS o llamada.

De igual manera mediante el ataque Torpedo se puede detectar la presencia de la víctima en cualquier área celular, esto siempre y cuando el atacante posea un rastreador en esa área.

## 5.4 Comparativa de como determina las amenazas existentes en redes móviles 4G y 5G

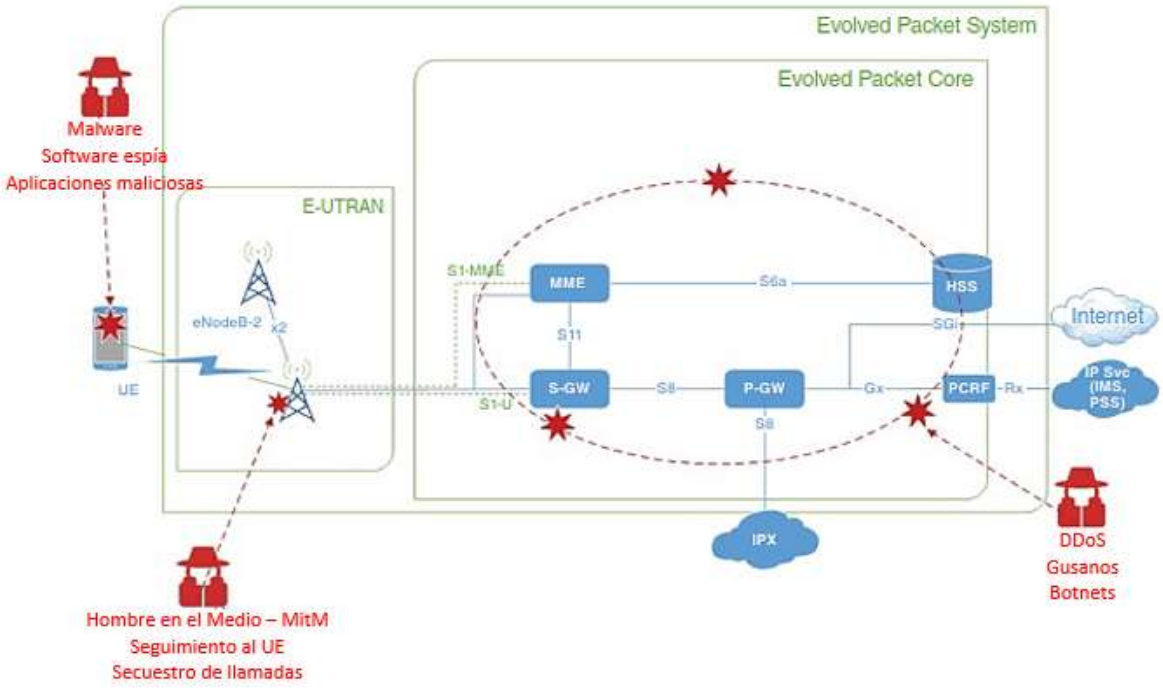
### *5.4.1 Amenazas existentes en redes móviles 4G*

Como se muestra en la Figura 3.4, las amenazas la red móvil de cuarta generación estaban esparcidas en múltiples dominios de la red 4G. Había nuevos tipos de virus y malware dirigidos a los teléfonos inteligentes con el fin de robar datos y contraseñas de los usuarios. Millones de aplicaciones maliciosas se han desarrollado para hacerse pasar por juegos de usuarios, utilidades o aplicaciones bancarias importantes falsas, de tal manera que los atacantes identificaron nuevas vulnerabilidades con la finalidad de desarrollar nuevas amenazas (Liyanage et al., 2020).

La amenaza a la seguridad en 4G LTE se pueden dar en las diferentes secciones de la arquitectura como el UE, RAN, Core Network y los servicios de internet como se puede observar en la Fig.28 que se describirán a continuación.

**Figura 28**

Panorama de amenazas a la seguridad 4G




*Fuente: Autor*

- **Amenazas a la seguridad en el Equipo de Usuario**

  Los teléfonos móviles siempre están conectados a una conexión inalámbrica o celular, donde los usuarios pueden acceder a sus datos en cualquier lugar y momento mediante el uso de aplicaciones. Hoy en día, la mayoría de nuestro tiempo se pasa en dispositivos móviles y a su vez en las aplicaciones las cuales conllevan a fallos de seguridad que poseen estas, ya que los usuarios o atacantes pueden descargar estas aplicaciones de forma intencionada o accidental. Se pueden instalar gusanos o malware y lanzar un ataque a la red de usuarios locales o a el proveedor de servicios, ya que estos consideran un teléfono móvil como dispositivo de red confiable. Su principal objetivo es obtener accesos a los datos personales y contraseñas del usuario que se encuentran almacenadas en el dispositivo móvil (Poot, 2022).
- **Amenazas a la seguridad de la Red de Acceso**

  En LTE-EUTRAN se puede vulnerar para obtener acceso a ubicaciones del UE utilizando su identificador temporal de red de radio celular(C-RNTI), ya sea que el UE resida en una celda o se desplace entre ellas.
- **Amenazas a la seguridad de la Red Central**

  Debido a que en LTE la comunicación de extremo a extremo se basa en IP abre la red móvil a amenazas de seguridad basadas en IP. La red central puede ser objetivo de un ataque de denegación de servicio distribuido (DDoS) generando un impacto como la perdida de servicios para millones de usuarios. Este ataque puede apuntar al (Envolved Packet Core) provocando una pérdida de servicio y desbordamiento del sistema. Un ejemplo es el ataque TCP SYN, en el que se envía un dispositivo de red con millones de paquetes TCP SYN falsos provocando una denegación de servicio y a su vez poder instalar malware.

  A continuación, en la Tabla 7 se describen las amenazas, su descripción, la gravedad del impacto al darse esta amenaza y su ocurrencia en la red móvil 4G.

**Tabla 7**
Riesgos a la seguridad en redes móviles 4G

| Amenaza | Descripción de la amenaza | Gravedad del impacto (Menor, Moderado, Severo, Extremo) | Amenaza, Ocurrencia (1-5, Bajo Alto) |
|---|---|---|---|
| Sistema Operativo móvil inseguro | Sistemas operativos móviles contienen vulnerabilidades que se solucionan mediante parches y actualizaciones. Estos provocan que atacantes puedan aprovechar las vulnerabilidades para piratear sistemas móviles | Moderado | 4 |
| Descargar aplicaciones móviles no autorizadas | Usuarios descargan aplicaciones que no se encuentran verificadas por el proveedor y contienen virus maliciosos | Moderado | 5 |
| Aplicaciones inseguras con datos confidenciales | Uso de aplicaciones que filtran datos personales y confidenciales sin ningún mecanismo de seguridad | Severo | 5 |
| Virus | Software malicioso con el objetivo de dañar archivos móviles | Severo | 2 |
| Malware | Virus avanzado que puede propagarse y que puede reproducirse con el objetivo de dañar datos a gran escala | Extremo | 3 |
| DDoS | Este es un ataque coordinado que involucra a cientos de dispositivos infectados con código malicioso, su objetivo es degradar la disponibilidad de la red | Extremo | 2 |
| Hombre en el Medio -MitM | Creación de estación base falsa para detectar el tráfico del UE y la estación base | Extremo | 2 |

*Fuente: Autor*

### *5.4.2 Amenazas existentes en redes móviles 5G*

El vector de amenaza para 5G puede ser amplio debido a su amplia gama de aplicaciones y servicios, así como a su papel fundamental en el servicio de la sociedad para el crecimiento social, económico y la seguridad pública. Las motivaciones para amenazar y atacar el 5G serán

mayores que en generaciones de redes anteriores. Existe una mayor probabilidad de que el 5G sea un objetivo clave para actividades criminales impulsadas por una variedad de motivos, incluidos motivos políticos patrocinados por el Estado, adversarios, cárteles del crimen organizado, espionaje y guerra cibernética.

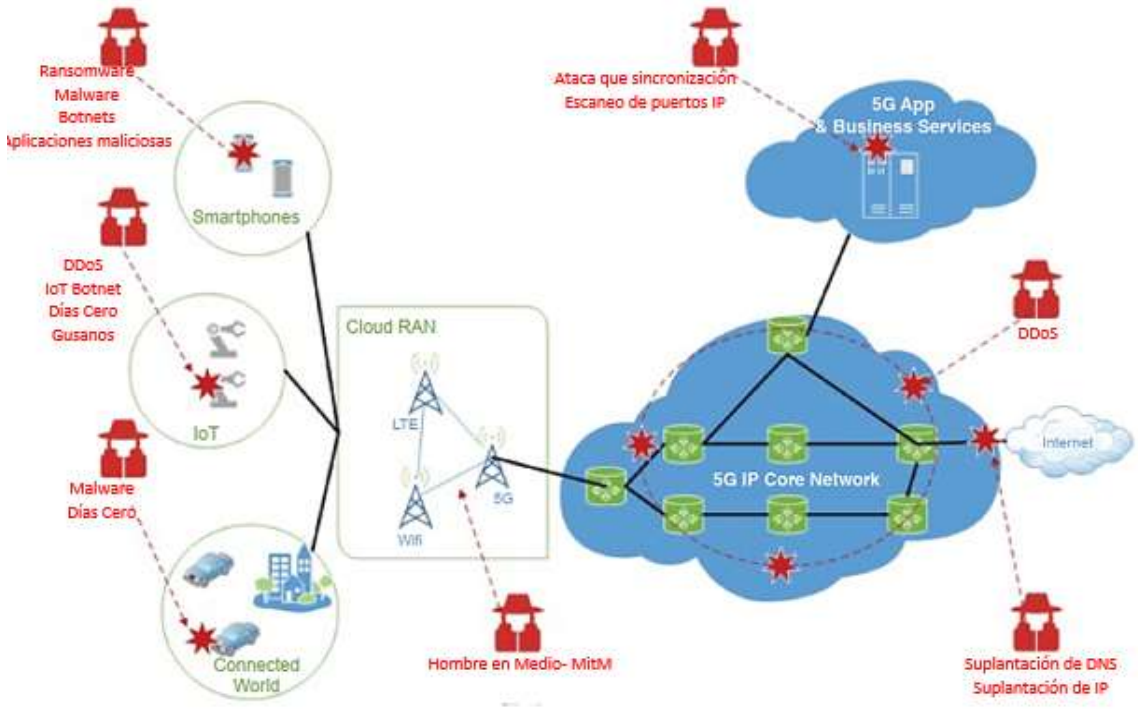
Los delincuentes continúan explorando nuevas formas de escapar de la detección, habiendo aprendido a explotar el sistema social y financiero para sus necesidades. Con la evolución de los sistemas de pago digitales y la incorporación de tecnologías como Bitcoin a la corriente principal, será mucho más sencillo para los delincuentes permanecer ocultos y seguir obteniendo beneficios financiero (Liyanage et al., 2020).

La amenaza a la seguridad en 5G se pueden dar en las diferentes secciones de la arquitectura como el UE, RAN, Core Network y los servicios de internet como se puede observar en la Fig.29 que se describirán a continuación.

En 5G los vectores de amenazas abarcaran desde los equipos de usuario, sensores, automotores automatizados y redes móviles. Estas amenazas abarcan desde los UE hasta la red de acceso por radio (RAN), pasando por la red central móvil e internet. La Fig.29 que nos muestra las amenazas incluidas como el ransomware, software espía, malware y bots. En un caso específico se podría lanzar un ataque MitM en la Cloud RAN, mientras que DDoS se puede usar en la red central IP (Poot, 2022).

**Figura 29**

Panorama de amenazas a la seguridad 5G




*Fuente: Autor*

A continuación, se describen algunas amenazas que se dan en cada bloque de las redes móviles 5G:

- **Amenazas a la seguridad en el Equipo de Usuario**

  Dispositivos vulnerables lo cual implica ataques de DDoS mediante varias solicitudes al servidor con la finalidad de denegar el acceso a los recursos de la red y vulnerando la integridad de los datos que se encuentran almacenados en el dispositivo.

- **Amenazas a la seguridad de la Red de Acceso**

  En la RAN las vulnerabilidades son aprovechados por ataques MitM el cual lanza ataques como; ataques de identificación, ataques de agotamiento de batería y captura de capacidades del dispositivo. La finalidad de este ataque es vulnerar la disponibilidad, integridad y confidencialidad de los dispositivos móviles que se conecten a la red móvil.

- **Amenazas a la seguridad de la Red Central**

  Debido al núcleo de la red en 5G que se basa principalmente en IP, se hereda la mayoría de amenazas de LTE que existen actualmente. El núcleo de la red 5G puede ser objetivo de un ataque de denegación de servicio distribuido (DDoS) generando el colapso y perdida de servicio para usuarios que deseen acceder a los servicios de la red móvil. De igual manera la red 5G se ve afectada por la suplantación de IP, donde los atacantes utilizan herramientas para modificar la dirección IP origen en la cabecera del paquete ya que el sistema que lo reciba cree que es un paquete confiable (Karpersky, 2023).

A continuación, en la Tabla 8 se describen las amenazas, su descripción, la gravedad del impacto al darse esta amenaza y su ocurrencia en la red móvil 4G.

**Tabla 8**

Riesgos a la seguridad en redes móviles 5G

| **Amenaza** | **Descripción de la amenaza** | **Gravedad del impacto (Menor, Moderado, Severo, Extremo)** | **Amenaza, Ocurrencia (1-5, Bajo Alto)** |
|---|---|---|---|
| Equipo de Usuario | Equipos vulnerables a DDoS e integridad de datos del dispositivo. | Severo | 3 |
| Secuestro de datos | Ransomware especializados cifran, bloquean y explotan el acceso a datos críticos. Se debe pagar dinero por el rescate de la información | Severo | 3 |
| Malware avanzado | Malware dirigido a millones de dispositivos móviles y de IoT | Extremo | 3 |
| Ataque de Hombre en Medio MitM | Ataque de identificación donde descubre los dispositivos conectados a la red y ataques de agotamiento de batería. | Extremo | 5 |
| Botnets de IoT | Dispositivos móviles e IoT alojan un agente/bot de control el cual recibe comandos remotos y filtra información de telemetría de un bot maestro. Estos se usan para ataques pasivos como activos | Severo | 2 |
| Amenazas a la infraestructura | Estas amenazas son enfocadas en dañar servicios de infraestructura críticos como SCADA | Extremo | 5 |

| | | | |
|---|---|---|---|
| Denegación de servicio Distribuido DDoS | Ataques de denegación debido a su mayor ancho de banda y pueden ser críticos en el núcleo de red. | Extremo | 5 |
| Ataques de día cero | Ataque avanzado que explota las vulnerabilidades no descubiertas de un sistema, este contempla una combinación de ataques como malware, ransomware y botnets | Moderado | 2 |

*Fuente: Autor*

### *5.4.3 Resumen de Vulnerabilidades en las redes móviles 4G y 5G*

En base a las investigaciones realizadas de las amenazas en redes 4G y 5G se han descubierto algunas vulnerabilidades que siendo empleadas por atacantes expertos pueden generar daños muy graves a las redes móviles. Dada la triada de la seguridad la cual está compuesta por la Confidencialidad, Integridad y Confidencialidad en la Tabla 9 se puede encontrar una descripción general de las amenazas y su impacto que genera en cada una de ellas, ya que es probable que esto se puedan resolver con el desarrollo de nuevos estándares que se desarrollen a fututo (Fonyi, 2020).

A continuación, en la Tabla 9 se describen el principio de seguridad, la amenaza y el impacto en caso de darse cualquier amenaza.

**Tabla 9**

Resume de las amenazas e impactos en 4G y 5G

| **Principio de Seguridad** | **Amenaza** | **Impacto** |
|---|---|---|
| Confidencialidad | Ataque al protocolo de autenticación AKA | Suplantación de identidad<br>Mensajes de fallo de autenticación |
| | Hombre en Medio - MitM | Creación de base falsa entre el UE y la estación base<br>Robo de claves de autenticación de sesión<br>Determinación de ubicación<br>Implementación de malware |
| Integridad | Hombre en Medio - MitM | Modificación o duplicación de mensajes |

| | | |
|---|---|---|
| | | Falsificación de UE para realizar llamadas o enviar mensajes<br>Degradación del canal de radio para obligar a conectarse a GSM |
| Disponibilidad | Denegación de servicio Distribuido - DDoS | Sobrecarga del sistema con solicitudes falsas<br>Tráfico de datos desde varios dispositivos a la vez<br>Implantación de software malicioso<br>Difícil de rastrear y ataque devastador a los sistemas. |

*Fuente: Autor*

### 5.5 Etapa III: Evaluación de nuevas tecnologías para la seguridad en redes 5G.

En este apartado se destacan las principales soluciones de seguridad para los desafíos de seguridad descritos en la sección anterior. La implementación de las nuevas tecnologías como radio definido por software (SDN) y la virtualización de funciones de red (NFV) que pueden resolver varios problemas de una mejor manera. En SDN, el controlador puede recolectar estadísticas a través de APIS desde el equipo de red con la finalidad de comprobar si aumentan los niveles de tráfico, así mismo con NFV los servicios de la red central pueden transferirse al borde para cumplir con los requisitos que necesita el usuario. De tal forma que las segmentaciones de la red se pueden dedicar a áreas con alta densidad de usuarios para hacer frente al tráfico que se genere (Liyanage et al., 2020).

En las redes 5G se deben implementar sistemas robustos de seguridad contra ataques con mayor garantía de privacidad y seguridad principalmente para la autenticación e identificación. Los mecanismos de seguridad flexibles deberán permitir el cifrado para el plano de usuario y los ajustes de los parámetros de seguridad por cada segmento de red.

Dado que en 5G tiene mayor flexibilidad y agilidad por lo tanto NFV y SDN son vitales para brindar seguridad en los sistemas 5G. A continuación, se describen cada una de ellas.

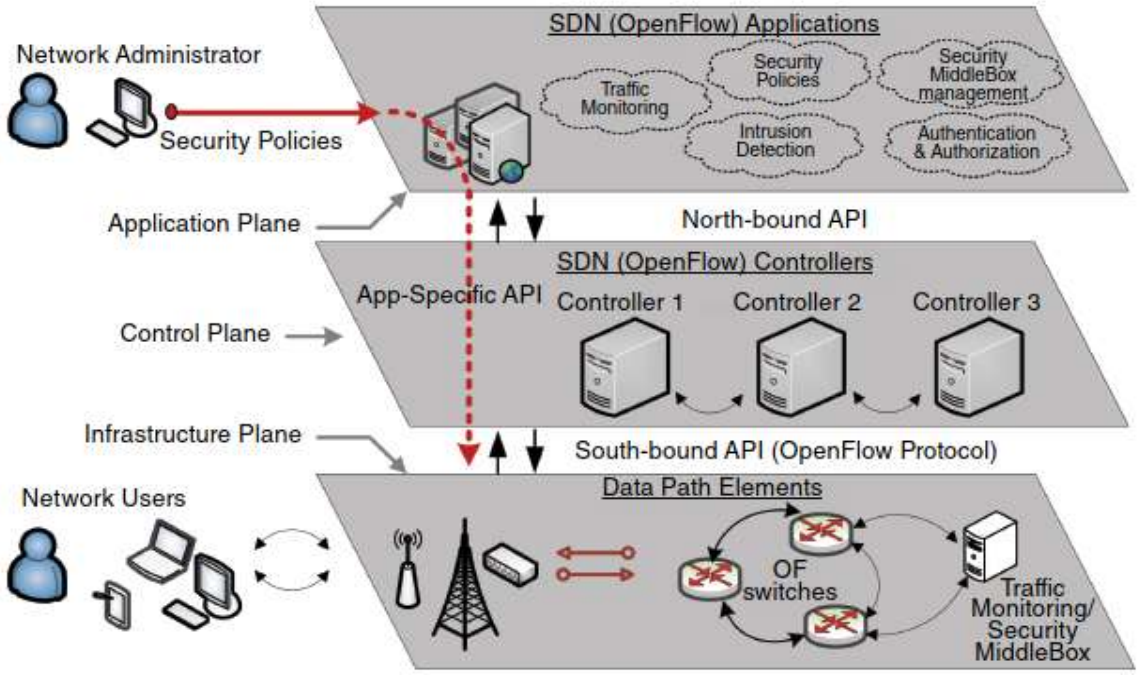
### *5.5.1 Redes definidas por Software (SDN)*

Las redes SDN (Software Defined Network) son un conjunto de técnicas relacionadas con el campo de las redes computacionales cuyo objetivo es facilitar la implantación e implementación de servicios de red de manera determinista, dinámica y escalable, lo que evita que los administradores de redes coordinen dichos servicios a nivel bajo. Por lo tanto, toda la inteligencia y la lógica de control de la red se han transferido desde los dispositivos de red a una entidad lógica basada en software (Fajardo & Cáceres, 2022).

Además, todas las operaciones de red deben describirse como programas de software integrando algoritmos, estructuras de datos y conceptos de programación que pertenecen al entorno de desarrollo de software, ya que las redes SDN incorporan el concepto de programabilidad de red. La seguridad de las redes de comunicación y de datos es un aspecto importante, por lo que estas redes pueden beneficiarse de las características de las redes SDN, como la programabilidad de la red. Esto permite que se cumplan las aplicaciones de software de seguridad de la red, SDN puede resolver varios problemas de seguridad que con frecuencia amenazan las redes convencionales de manera oportuna y confiable.

**Figura 30**

Arquitectura SDN




*Fuente: (Liyanage et al., 2020)*

Como se puede observar en la Fig. 30 la virtualización de redes se compone de tres capas; la capa de aplicaciones, la capa de control y la de infraestructura, las cuales están conectadas mediante API de comunicación ascendente como descendente que a continuación se describe la funcionalidad de cada una de ellas.

- **Capa de Aplicaciones**

  Todas las aplicaciones y funciones de red que solicita el usuario se encuentran en esta capa y se comunican con la capa de control a través de la API Northbound (hacia arriba). Esto permite simplificar y automatizar las tareas de configuración, ofrecer servicios y proporcionar ingresos diferenciados al usuario según el perfil del usuario y el servicio que vaya a consumir, recopilar estadísticas que reflejan su comportamiento en la red y luego tomar decisiones. asegurando su seguridad y portabilidad porque funciona con todos los sistemas operativos (Tapiero et al., 2021)

- **Capa de Control**

  En esta capa se administran las políticas y el flujo de tráfico por la red ya que consta de del controlador OpenFlow que toma decisiones en la capa de control en la red SDN, ya

que esta conecta la capa de aplicaciones a la de infraestructura a través de la API Southbound (hacia abajo) y luego las pasa a la infraestructura de red actual a través de la API Southbound (hacia arriba) a la capa de control como se puede observar en la Fig.30. También es la encargada de comunicar la información extraída de la capa de infraestructura de vuelta a la capa de aplicación para optimizar la funcionalidad

- **Capa de Infraestructura**
  También conocido como capa de datos, está compuesto por nodos que se encargan de la conmutación y encaminamiento de paquetes, reemplazando a dispositivos de red como interruptores, routers y puntos de acceso que eran responsables de la transmisión de datos por la red. La capa de control puede reprogramar esta capa utilizando la API OpenFlow para configurar la funcionalidad de la capa de datos en modo de rutero o firewall según sea necesario.

### *5.5.2 Soluciones de seguridad en redes móviles 5G basadas en SDN*

El plano de control de SDN admite el monitoreo de seguridad, análisis de tráfico y sistemas de respuesta que son altamente efectivos y proactivos con la finalidad de facilitar el análisis forense de la red, la alteración de la política de seguridad y la inserción de servicios de seguridad.

SDN facilita una identificación rápida de amenazas que pueden darse a través de un ciclo inteligente de recopilación de recursos, estados y flujos de la red. En la arquitectura de la SDN se da la redirección de tráfico mediante el uso de tablas de flujo para analizar los datos, actualizar la política y reprogramar la red en consecuencia. Así mismo el uso de la programabilidad facilita la implementación de políticas de seguridad sin la necesidad de configuración de hardware (Revelo & Morales, 2021).

A continuación, se describen la seguridad que emplea en cada plano o capa en SDN:

- **Seguridad en el Plano de Aplicación**

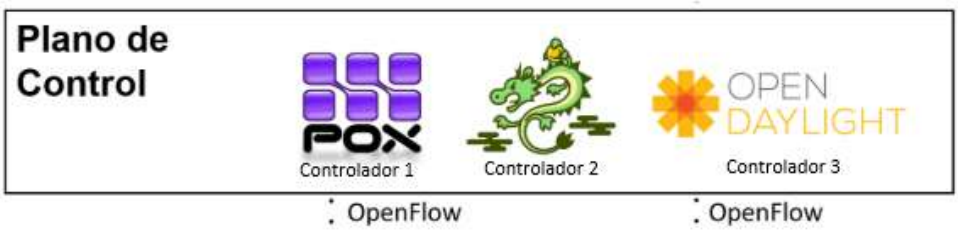
**Figura 31**
Plano de Aplicación


*Fuente: Autor*

La arquitectura de control facilita el uso de varias aplicaciones a las cuales les proporciona estadísticas de la red y características de los paquetes para implementar nuevos servicios de seguridad. El sistema PermOF facilita el acceso controlado a los datos y planos de control de las aplicaciones SDN, este sistema proporciona permisos de lectura, escritura y notificación a varias aplicaciones para hacer cumplir los permisos de control. Esto permitirá la protección de los datos, poniendo a buen recaudo la integridad de la información ya que la SDN permite que varias aplicaciones implementen medidas de seguridad de extremo a extremo para la seguridad de la red.

- **Seguridad en el Plano de Control**

**Figura 32**
Plano de Control




*Fuente: Autor*

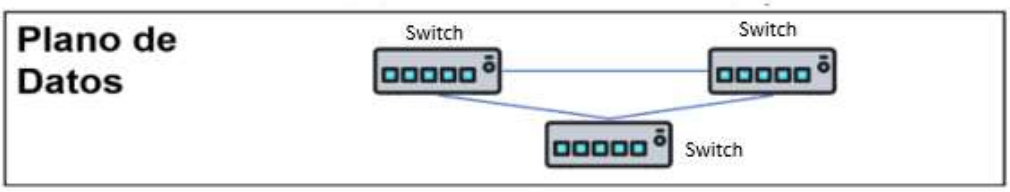
La seguridad en el plano de control es fundamental para toda la red es por ello que se emplea el controlador SE-Floodlight el cual proporciona mecanismos para la separación de privilegios al agregar una API programable y segura con dirección hacia arriba del controlador y opera como medidor ente la aplicación y el plano de infraestructura, además verifica todas las reglas de flujo que se generan por las aplicaciones y resuelve conflictos de reglas de flujo entre ellas. Para mitigar las

amenazas al controlador y los posibles ataques de DoS debido a su función centralizada, se usan estrategias de resiliencia de controlador. Estas estrategias incluyen resiliencia del controlados a través de la redundancia, maximizando capacidades de almacenamiento y procesamiento del controlador entre múltiples puntos de la red empleando técnicas de equilibrio de carga entre varios controladores en una red.

- **Seguridad en el Plano de Infraestructura**

**Figura 33**

Plano de Infraestructura




*Fuente: Autor*

En este plano debe estar protegido contra aplicaciones no autorizadas, ya que estas aplicaciones pueden instalar, modificar o cambiar las reglas de flujo en el plano de infraestructura o datos por lo cual se usan mecanismos de seguridad como autenticación y autorización solamente para las aplicaciones que pueden cambiar las reglas de flujo en el plano de datos. Un ejemplo es ForntNox que permite al controlador verificar las contradicciones en las reglas del flujo generadas por las aplicaciones (Revelo & Morales, 2021).

A continuación, se describen las medidas de protección ante las amenazas en 5G.

**Tabla 10**

Medidas de protección ante amenazas en 5G

| Amenazas | Medidas de protección |
|---|---|
| Equipo de Usuario | Implementación de autenticación solida es una solución para este tipo de ataque.<br>Uso de SDN para una mejor autenticación de manera rápida, flexible y programable |
| Ataque Hombre en el Medio MitM | Seguridad para la integridad en el plano de usuario mediante el controlador SE-Floodlight que proporciona mecanismos para la separación de privilegios al agregar una API programable que funciona como mediador entre la aplicación y el plano de datos. |
| Amenazas a la RAN | Uso del identificador SUPI que evita que un atacante rastree un objetivo que afecte la privacidad del UE |

| | |
|---|---|
| | Uso de MIMO que garantiza la integridad de la información operando en el espectro de onda milimétrica. |
| SDN y NFV | Uso de túneles Ipsec<br>Protección contra la selección fraudulenta de segmentos de red.<br>Evitar acceso no autorizado a los segmentos de red<br>Uso de varios procedimientos de autenticación y autorización de usuarios a los segmentos.<br>Aislamiento de los segmentos de red, incluso si el mismo UE está conectado a ambos al mismo tiempo. |
| Denegación de Servicio -DoS | Protección contra ataques de DoS contra los recursos compartidos en los diferentes sectores.<br>Autenticación robusta con mayor flexibilidad y programabilidad.<br>Seguridad en los puntos de control centralizados. |

*Fuente: Autor*

### *5.5.3 Mitigación de ataques mediante la SDN*

Existen posibilidades de implementar estrategias de mitigación de amenazas que se adapten a las características de la arquitectura SDN, como son la programabilidad de la red y la gestión centralizada de flujos, ya que la mayoría de amenazas se seguridad que se observan normalmente en las redes convencionales pueden darse en escenarios SDN. Debido a que los controladores tienen acceso total a toda la información sobre el estado de la red, se pueden implementar numerosas soluciones de control. La aplicación puede ordenar al controlador que emita las entradas de flujo adecuadas para corregir cualquier comportamiento desviado.

Por ejemplo, una aplicación de mitigación de ataques SDN podría incluir un módulo de reacción que aplica directamente un conjunto de acciones de mitigación a los elementos de red comprometidos (flujos, switches, canales, interferencias, etc.) y un mecanismo de detección que sea capaz de distinguir características específicas de un comportamiento irregular de la red de acuerdo con características específicas descritas en un conjunto de políticas de seguridad (Ruipérez, 2021). A continuación, se detallarán algunos métodos de mitigación basados en SDN para diferentes tipos de ataques a la seguridad:

- **Ataques de denegación de servicio DoS o DDoS**

  Para mitigar este tipo de ataques en las redes SDN se necesita de gestión y aplicación de políticas de red de alto nivel, las cuales debe estar almacenadas en un repositorio y

puedan traducirse en rutas para redistribuir los flujos de ataque y aliviar en gran medida la congestión en los enlaces. Tras la detección de anomalías, los clientes darán una alerta de aviso a un componente de supervisión de la red conectado al controlador del proveedor de servicio de internet y luego el componente de vigilancia pueda extraer la información de las diferentes rutas que se encuentran congestionadas, solicitando a la base de datos de políticas que acciones deben tomarse contra el ataque (Tapiero et al., 2021)

- **Infiltración de dispositivos de control de acceso**

  Para defender las redes SDN del control de acceso una solución es Network Flow Guard (NFG) la cual se encarga de los ataques de intrusos ilegales que se infiltran en las redes aprovechando puntos de acceso inseguros desplegados intencionalmente en la topología de red. NFG realiza la detección de los puntos de acceso fraudulentos basándose en un esquema de inspección pasiva de paquetes combinado con un sistema de detección activa (Ruipérez, 2021)

- **Gestión de acceso y de la identidad del usuario**

  En las redes SDN la información sensible se trasmite por el plano de control, por lo que muchos ataques MitM se centran en espiar este canal de control con la finalidad de obtener la información suficiente para poder comprometer la red. La seguridad empleada es el uso de aplicaciones de cifrado en los canales de comunicación de extremo a extremo ya que, aunque los atacantes puedan filtrar los datos cifrados no podrán tener los datos en texto plano.

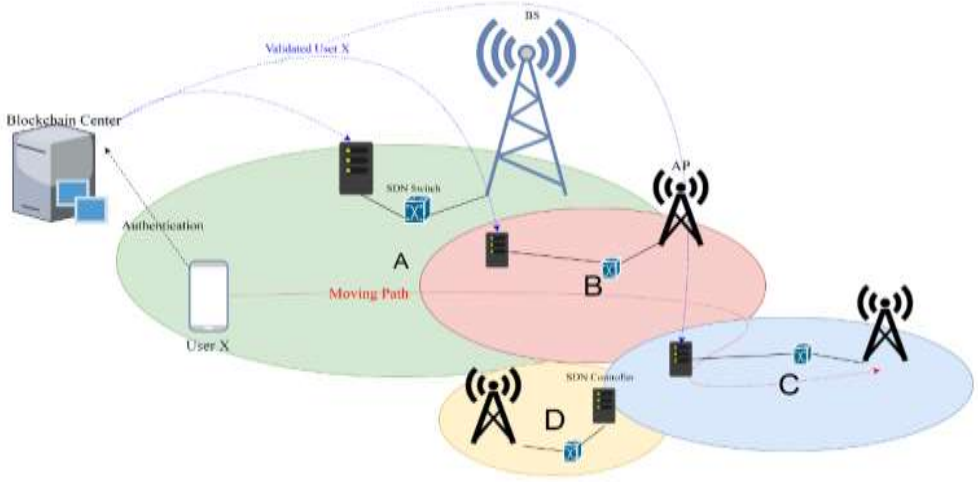
## 5.6 Etapa IV: Recomendaciones y medidas de seguridad en las redes 5G

### *5.6.1 Autenticación basada en Blockchain para redes 5G*

El objetivo del caso de estudio se basa en diseñar e implementar un protocolo de autenticación mediante el uso de clave y seguro utilizando la tecnología blockchain con la finalidad de mejorar la seguridad en las redes móviles 5G (Haddad et al., 2020).

Hoy en día se han identificado varias vulnerabilidades en los protocolos existentes como ataques de suplantación de identidad, denegación de Servio DoS, denegación de servicio distribuido (DDoS) y el ataque hombre en el Medio (MitM).

**Figura 34**
Tecnología Blockchain en 5G




*Fuente: Autor*

La tecnología blockchain se ha convertido en una solución potencial para abordar estos problemas de seguridad. La cadena de bloques puede brindar una mayor protección en el proceso de autenticación y acuerdo de clave gracias a sus características de seguridad inherentes, como la confidencialidad, la integridad y la distribución de la base de datos.

En su trabajo de investigación (Haddad et al., 2020) desarrollan un nuevo protocolo de registro y autenticación basado en blockchain para redes 5G con la implementación de técnicas criptográficas como la firma digital, sellos de tiempo y emparejamiento bilineal con la finalidad de proteger el protocolo propuesto de los ataques identificados anteriormente.

Este protocolo de registro y autenticación utiliza una baja potencia computacional y una cantidad pequeña de paquetes, reduciendo la sobrecarga de comunicación y computación preservando el consumo de batería debido a un bajo proceso de cómputo. A continuación, se describen tres análisis de seguridad empleando blockchain:

- **Seguridad basada en Blockchain**

  La cadena de bloques protege la red 5G contra ataques de secuestro porque se distribuye por toda la red y la clave pública está completamente registrada, validada y verificada. Los ataques de secuestro no pueden obtener información de un nodo y usarla en otro. Esto garantiza la integridad de los datos distribuidos ya que nadie podrá modificar o eliminar el bloque o la transacción de blockchain.

- **Seguridad basada en firmas**

  Del esquema propuesto cada nodo de la red, ya sea el UE posee una clave pública y privada generada a partir de la red domestica (HN). La red domestica registra la clave publica en la cadena de bloques, por lo que no existe la posibilidad de falsificar la clave pública ayudando a mejorar la escalabilidad, la eficiencia y resiliencia de la red.

- **Seguridad basada en marcas de tiempo**

  Estas marcas de tiempo son usadas con la finalidad de frustrar los ataques de reducción de paquetes, donde cada nodo debe verificar las marcas de tiempo para saber que el paquete este actualizado, ya que si no se pueden identificar el paquete obsoleto este no se retransmitirá (Haddad et al., 2020).

En conclusión, se debe considere la privacidad de los usuarios, aunque el método de autenticación y acuerdo de clave basado en blockchain ofrece seguridad y autenticidad, es importante tener en cuenta la privacidad de los usuarios. Se pueden considerar técnicas criptográficas y de anonimización para asegurarse de que la información personal y los datos sensibles estén protegidos y solo sean accesibles por las entidades autorizadas.

### *5.6.2 Mecanismos de seguridad para mitigar ataques de señalización DoS basados en RRC y asegurar la disponibilidad.*

La protección del enlace de radio 5G con los dispositivos no debe ser descuidado en favor de dar mejores características más atractivas y capacidades novedosas. La información fundamental del sistema, como los mensajes del bloque de información del sistema (SIB) debe comunicarse a los dispositivos 5G mediante un canal de radio cifrado y con integridad protegida. Además, para aumentar la seguridad del RRC los dispositivos 5G deben actualizarse

periódicamente y dotarse de soluciones antimalware y antivirus básicos para identificar aplicaciones maliciosas. Las herramientas de seguridad modernas deben emplear un alto grado de inteligencia para operar de manera autónoma y proactiva frente a estas amenazas (Ettiane et al., 2021).

### *5.6.3 Posibles impactos y recomendaciones de seguridad en redes móviles 4G*

Es evidente que un ataque MitM tendría un impacto en la disponibilidad, la integridad y la confidencialidad de la información, ya sea a través de la red de telecomunicaciones o directamente en Android. Algunas de las consecuencias podrían ser:

- Perdida de disponibilidad: No se podría tener conexión con las antenas cercanas desde el dispositivo móvil, y no se podría realizar llamadas.
- Perdida de Confidencialidad: Permite a un atacante robar datos técnicos o personales porque las tramas y los datos enviados se pueden visualizar, lo que supone una violación clara de la intimidad si los datos obtenidos representan a las personas.
- Perdida de integridad: Si se consigue una copia de la información, los datos se podrían alterar o acceder al sistema a través de la red móvil, sea esta por fuerza bruta, ingeniería social o explotando una vulnerabilidad del sistema operativo del equipo celular.
- Con la finalidad de reducir estos riesgos es necesario que los usuarios móviles tengan configuradas las protecciones de los proveedores móviles y la instalación de antivirus.

En conclusión, un atacante con pocos recursos podría capturar el tráfico de las redes móviles y usarlo para fines maliciosos. Por lo tanto, conocer el funcionamiento de la tecnología de telecomunicaciones en relación con el uso y las amenazas de seguridad permite, con las herramientas adecuadas (administrativas y técnicas), vulnerar el sistema y obtener información valiosa, tanto en tránsito como local (Roldán & Vargas, 2020).

### *5.6.4 Análisis de resultados y mejoras en seguridad para salvaguardar la integridad*

En 5G se puede realizar el uso del ataque IMSI Catcher siempre y cuando el teléfono móvil tuviera la capacidad para usar las bandas 5G adecuadas. Cuando el UE se conecta a una red 5G utilizara el procedimiento de LTE donde enviara el IMSI en texto claro si es la primera vez que se conecta a dicha red.

Esta vulnerabilidad es muy crítica ya que obteniendo el IMSI se podría localizar al abonado vulnerando la confidencialidad e integridad del mismo.

Como seguridad las operadoras en 5G deberán considerarán la virtualización al desarrollar su infraestructura. Tanto SDN como NFV son tecnologías complejas y prematuras de desarrollar, aunque es cierto que esto reduce significativamente los costos. Además, debido a las infinitas posibilidades en el despliegue, no existen estándares que las operadoras puedan seguir para implantar su infraestructura. Entonces, la implementación de estas tecnologías de virtualización sigue siendo incierta (Gallego, 2021).

### *5.6.5 Recomendación de seguridad para la disminución del ataque TORPEDO*

De igual manera mediante el ataque Torpedo se puede detectar la presencia de la víctima en cualquier área celular, esto siempre y cuando el atacante posea un rastreador en esa área.

A continuación, se describen las mejoras en la seguridad para prevenir estos ataques torpedo:

- Se debe frustrar la causa raíz de Torpedo garantizando que la búsqueda de un UE no permanezca fija en un área de celda particular.
- Hacer que primero la búsqueda dependa del TMSI en vez del IMSI puede ser una buena solución
- Se debe garantizar que el TMSI de un UE se reasigne después de recibir un mensaje de localización
- Introducir la aleatoriedad para garantizar que el UE como el eNodeB y el MME compartan una fuente común aleatoria a partir de la cual se deberán generar números pseudoaleatorios que se usaran como identificador y ocasión de búsqueda.

Finalmente, en la Tabla 11 se describen los requisitos de seguridad que se deben tomar en cuenta en los elementos de la red móvil 5G.

**Tabla 11**

Requisitos de seguridad para elementos de Red 5G

| **Elementos o Funciones de red 5G** | **Requerimientos de seguridad** |
|---|---|
| UE | Cifrado de señalización y datos entre el UE y gNB por temas de confidencialidad.<br>Garantizar la integridad de los datos para la señalización y los datos de usuario entre el UE y el gNB<br>Almacenamiento de SUCI (Identificador oculto de suscripción) |
| gNB | Procesamiento y almacenamiento seguro de datos de usuario y señalización<br>Proporcionar un entorno seguro para todos los datos confidenciales.<br>Protección de claves utilizadas y almacenadas en el gNB<br>Garantizar la integridad de los datos para la señalización y los datos de usuario entre UE y gNB |
| AMF | Debido al cifrado de confidencialidad de la señalización NAS<br>Garantizar la integridad de los datos para la señalización NAS |
| SEAF | Activa la autenticación a través de AMF en la red de servicio<br>Admite la autenticación primaria del UE |
| UDM | Las claves a largo plazo para la autenticación deben estar protegidas y no deben salir del entorno UDM/ARPF (repositorio de credenciales de autenticación y función de procesamiento) |
| AUSF | Procesamiento de solicitudes de autenticación para acceso<br>Transfiere el SUPI a la red telefónica publica después de la autenticación exitosa |
| Red Principal | Creación de zonas de confianza para distintos proveedores móviles<br>Descubrimiento seguro y registro de NF en la SBA<br>Conexiones seguras de extremo a extremo para la capa de aplicación entre redes centrales 5G |

*Fuente: Autor*

De acuerdo a cada elemento de la red móvil en 5G se debe tener requerimientos de seguridad con la finalidad de que la comunicación sea segura para el usuario que está haciendo uso de la red móvil.

## 6. Discusión

El análisis comparativo de la seguridad de redes móviles 4G y 5G que se ha desarrollado en esta investigación ha permitido determinar las principales vulnerabilidades y riesgos que pueden darse al ejecutarse un ataque a estas tecnologías. Estos desafíos de seguridad respaldan al objetivo general como específicos al descubrir las principales amenazas y como mitigarlas en estas redes móviles con la finalidad de brindar seguridad a los usuarios.

En un inicio se aborda un marco teórico referente a la evolución de las redes móviles, su arquitectura y sus principales características. De igual manera se hace mención a la seguridad empleada en cada generación de la red móvil con la finalidad de definir como han venido evolucionado las amenazas en cada generación celular.

Se realizo un análisis de las amenazas o vulnerabilidades de seguridad que afectan a las redes móviles 4G y 5G. Esto permitió comprender más acertadamente los desafíos de seguridad que deben tomarse en cuenta, con la finalidad de brindar mejores controles de seguridad para garantizar la confidencialidad, integridad, disponibilidad de tal modo que la red pueda ofrecer a los usuarios una plataforma de comunicación segura.

De acuerdo al análisis de la investigación, se evaluó la efectividad de las medidas de protección existentes en estas redes móviles 4G y 5G de acuerdo a varios casos de estudio, así como la gravedad de dicha amenaza y la ocurrencia de que se puedan dar. Estas evaluaciones permitieron determinar las principales amenazas y vulnerabilidades ya que siendo bien ejecutadas pueden lograr la no disponibilidad de los servicios de telecomunicaciones.

Como resultado, se planteó varias mejoras y medidas concretas en la seguridad de la red móvil 5G cumpliendo con los objetivos planteados en un inicio. Estas mejoras incluyen el uso de tecnologías de radio definido por software, así como la virtualización de las funciones de red y el uso de tecnología blockchain. El objetivo de estas mejoras en la red móvil 5G son una solución potencial que garantiza la seguridad y la privacidad en la comunicación de los usuarios manteniendo la disponibilidad, confidencialidad e integridad de los datos en una comunicación móvil.

## 7. Conclusiones

Las nuevas redes 5G permiten el desarrollo de nuevas aplicaciones y mejoras notables en términos de velocidad, latencia y capacidad en comparación con las tecnologías de redes celulares anteriores, pero también enfrentan nuevos desafíos de seguridad que deben abordarse adecuadamente. Dada la naturaleza de la tecnología, la disponibilidad, la confidencialidad y la integridad de datos son algunos de los grandes desafíos de las redes móviles 4G y 5G.

Los análisis realizados respecto a la seguridad de las redes 4G y 5G en los estudios presentados revelan la importancia de abordar varios desafíos que estas redes enfrentan con la finalidad de mantener segura la comunicación y asegurar la disponibilidad de los servicios cuando el usuario requiera. Las vulnerabilidades en los protocolos de autenticación y cifrado, como las identificadas en el protocolo de autenticación AKA de 4G, pueden comprometer la privacidad de los usuarios y permitir ataques de interceptación y suplantación de identidad.

A medida que avanza la tecnología, se requieren nuevos requisitos de seguridad y estudios para enfrentar tanto ataques conocidos como ataques aún por descubrir. La implementación de mecanismos de seguridad avanzados, como el cifrado de extremo a extremo, la autenticación mutua y la protección contra amenazas emergentes, como los ataques de denegación de servicio distribuidos (DDoS), es fundamental para garantizar la integridad, confidencialidad y disponibilidad de las redes 4G y 5G.

La virtualización de red y el uso de las redes definidas por software SDN pueden usarse junto con una variedad de protocolos para facilitar la gestión y protección de grandes flujos de datos con el objetivo de resguardar a los usuarios en la red móvil 5G. El uso de la tecnología blockchain se destaca como una solución prometedora ya que es fundamental adoptar un enfoque de seguridad proactivo y basado en el riesgo, que implique la evaluación continua de amenazas para garantizar la privacidad, la eficiencia y la confianza que se necesita para que los usuarios puedan comunicarse de una manera segura.

## 8. Recomendaciones

Para ampliar el análisis de la seguridad de las redes 4G y 5G se recomienda realizar una investigación más profunda y pruebas de seguridad mediante el uso de simuladores de redes móviles para validar su eficacia y funcionalidad de la red referente a la disponibilidad de los servicios en 5G.

Evaluar la eficacia de los mecanismos de seguridad en ambas redes frente a diferentes tipos de amenazas, como ataques de denegación de servicio distribuidos (DDoS), interceptación de tráfico, suplantación de identidad y vulnerabilidades en protocolos con el uso de herramientas de simulación.

Realizar un análisis exhaustivo de los desafíos de seguridad específicos que plantea la arquitectura descentralizada y virtualizada de las redes 5G, así como las implicaciones de la segmentación de la red y el aislamiento de los componentes virtuales cuando la red se vea comprometida por algún ataque.

Efectuar una investigación más detallada con el ánimo de abordar el uso de la tecnología blockchain ante los posibles desafíos de seguridad como la denegación de servicio, hombre en el medio, ataques de secuestro de información y validar que tan efectiva es la seguridad de la red empleando estos nuevos métodos de seguridad, con la finalidad de asegurar la disponibilidad, confidencialidad e integridad dentro de la comunicación móvil.

## 9. Bibliografía


Adewumi, A., Chizea, F., & Ayantunji, B. (2020). *Network and Complex Systems A Review of Cellular Networks: Applications, Benefits and Limitations*. *11*. https://doi.org/10.7176/NCS/11-04

Analuisa, M. J. D. (2014). *Diseño de una red 4G Long Term Evolution (LTE) en redes móviles* [bachelorThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones]. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/7796

Arcotel. (2020). *Agencia de Regulación y Control de las Telecomunicaciones—Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios.* Agencia de Regulación y Control de las Telecomunicaciones - Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios. https://www.arcotel.gob.ec/

Arcotel,2024. (s. f.). Lineas Activas—Agencia de Regulación y Control de las Telecomunicaciones. *Agencia de Regulación y Control de las Telecomunicaciones - Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación eficiente del espectro radioeléctrico y los servicios.* Recuperado 15 de marzo de 2024, de https://www.arcotel.gob.ec/lineas-activas/

Calderón, C. L. (2023). *Concientización en técnicas de anti phishing al personal administrativo de Universidad Nacional de Loja, mediante el uso de la herramienta GoPhish.* [masterThesis, Universidad Nacional de Loja]. https://dspace.unl.edu.ec//handle/123456789/26984

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

Cruz, M. H. J. (2022). *Análisis de riesgo y oportunidad de la implementación del sistema de telefonía móvil 5G en el Ecuador.* http://repositorio.ucsg.edu.ec/handle/3317/18011

Ettiane, R., Chaoub, A., & Elkouch, R. (2021). Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions. *Journal of Information Security and Applications*, *61*, 102943. https://doi.org/10.1016/j.jisa.2021.102943

Fajardo, C. A., & Cáceres, J. E. (2022). *Arquitectura y funcionamiento de redes definidas por software (SDN)*. http://repository.udistrital.edu.co/handle/11349/29727

Fernández, X. (2022). *Implementación de un prototipo de receptor para canal PDSCH de 5G NR sobre dispositivo comercial de bajo coste RTL-SDR.*

Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *Journal of Network and Computer Applications*, *101*, 55-82. https://doi.org/10.1016/j.jnca.2017.10.017

Flores Erazo, C. F. (2022). *Estudio de la infraestructura y el espectro radioeléctrico en la evolución de la tecnología 4G y su convergencia a 5G en redes de telefonía móvil en el Ecuador* [bachelorThesis]. http://repositorio.utn.edu.ec/handle/123456789/13357

Fonyi, S. (2020). Overview of 5G Security and Vulnerabilities. *Army Cyber Institute*, 21.

Fuentes, M. B., & Ibáñez, E. D. (2019). Tecnología móvil 5G. *Mare Ingenii*, *1*(1), Article 1. https://doi.org/10.52948/mare.v1i1.182

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

García, B. J. (2019). *Tecnologías 3G, 4G y 5G: Una perspectiva económico y social de la carrera por la innovación de las redes de banca ancha*. https://repositorio.comillas.edu/xmlui/handle/11531/27633

Garcia, G. (2020). Seguridad en dispositivos móviles: Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos. *20-01-2020*. https://openaccess.uoc.edu/bitstream/10609/107326/6/mgarciagarcia45TFM0120memoria.pdf

Gutierrez, M. B. M. (2021). *ANÁLISIS COMPARATIVO ENTRE LAS REDES 4G; 5G Y SU INFLUENCIA EN LA PARROQUIA URBANA SAN LORENZO DEL CANTÓN JIPIJAPA* [bachelorThesis, Jipijapa.UNESUM]. http://repositorio.unesum.edu.ec/handle/53000/2828

Haddad, Z., Fouda, M. M., Mahmoud, M., & Abdallah, M. (2020). Blockchain-based Authentication for 5G Networks. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 189-194. https://doi.org/10.1109/ICIoT48696.2020.9089507

Karpersky. (2023, abril 19). *Suplantación de IP: Cómo funciona y cómo prevenirla*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ip-spoofing

Liyanage, M., Ahmad, I., Abro, A. B., Gurtov, A., & Ylianttila, M. (Eds.). (2020). *A Comprehensive Guide to 5G Security* (1.ª ed.). Wiley. https://doi.org/10.1002/9781119293071

Lopa M & Vora, L. J. (2015). EVOLUTION OF MOBILE GENERATION TECHNOLOGY: 1G TO 5G AND REVIEW OF UPCOMING WIRELESS TECHNOLOGY 5G. *International Journal of Modern Trends in Engineering and Research*. https://www.semanticscholar.org/paper/EVOLUTION-OF-MOBILE-GENERATION-TECHNOLOGY%3A-1G-TO-5G-Vora/82bb15f1dcc9bf669601d3957cbe9b6178eab097

Muñoz, C. P. S. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/20932

Orange. (s. f.). *¿cómo funciona una red móvil? - Las ondas*. https://radio-waves.orange.com/. Recuperado 13 de marzo de 2024, de https://radio-waves.orange.com/es/como-funciona-una-red-movil/

Ortega, E. M. I. (2010). La telefonía móvil de cuarta generación 4G y Long Term Evolution. *Ingenius*, *4*, 3-12.

Oviedo, I. J. I. (2022). *Diseño de red móvil para optimizar la cobertura del sector Pepa de Huso, cantón Montecristi de la provincia de Manabí mediante Walktest.* [Universidad de Guayaquil. Facultad de Ingeniería Industrial. Carrera de Ingeniería en Teleinformática.]. http://repositorio.ug.edu.ec/handle/redug/59627

Poot, J. E. (2022). *Seguridad en redes 5G.* [bachelorThesis, Universidad Autonoma del Estado de Quintana ROO]. http://risisbi.uqroo.mx/handle/20.500.12249/2956?show=full

Rafiul, & Bertino. (2020). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. *NDSS Symposium*. https://www.ndss-symposium.org/ndss-

paper/privacy-attacks-to-the-4g-and-5g-cellular-paging-protocols-using-side-channel-information/

Redacción, T. y. (2023, junio 1). *Claro y Movistar negocian su continuidad en Ecuador: ¿cuántos clientes tiene cada operadora?* www.ecuavisa.com. https://www.ecuavisa.com/noticias/ecuador/telecomunicaciones-claro-movistar-vianna-maino-ML5278482

Revelo, D. A., & Morales, S. M. (2021). *Análisis y evaluación de la virtualización de redes Inalámbricas con SDN*. http://repository.udistrital.edu.co/handle/11349/28678

Rojo, B. A. (2021). *Seguridad en dispositivos móviles*. https://uvadoc.uva.es/handle/10324/50049

Roldán, M. Á. Á., & Vargas, H. F. M. (2020). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. *Ingeniería y Desarrollo*, *38*(2), 279-297.

Ruipérez, J. (2021). *Seguridad en Redes definidas por software (SDN)* [Proyecto/Trabajo fin de carrera/grado, Universitat Politècnica de València]. https://riunet.upv.es/handle/10251/165154

Taipe, S. G. M. (2022). *Diseño de la infraestructura de una red 5g para la ciudad de Ambato* [bachelorThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Electrónica y Comunicaciones]. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/36148

Tapiero, R., Gonzalez, A., & Novoa, N. (2021). Seguridad en redes SDN y sus aplicaciones. *REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA)*, *1*(37), Article 37. https://doi.org/10.24054/rcta.v1i37.1262

Telégrafo, E. (2020, febrero 6). *Tuenti alcanzó el 9% del mercado ecuatoriano en cuatro años*. El Telégrafo. https://www.eltelegrafo.com.ec/noticias/economia/1/tuenti-mercado-ecuador

Toro, R. (2021, marzo 11). ¿Qué es la seguridad de la información y cuantos tipos hay? *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Viavi. (2023, marzo 13). *Arquitectura de las redes 5G. Núcleo de red, redes RAN y arquitectura de seguridad para la tecnología 5G*. https://www.viavisolutions.com/es-mx/que-es-la-arquitectura-de-la-tecnologia-5g

# 10. Anexos

## Anexo 1. Certificación de traducción del resumen

Loja, 10 de junio de 2024

**CERTIFICADO DE TRADUCCIÓN**

Licenciado
Marco Patricio Guarnizo Cortez
LICENCIADO EN CIENCIAS DE LA EDUCACIÓN MENCIÓN IDIOMA INGLES

**CERTIFICO:**

Haber realizado la traducción de español a ingles del resumen de la tesis titulada **"Análisis comparativo entre la seguridad empleada en redes 4G y redes 5G"** de autoría de **JANDRY DARIO GONZÁLEZ GONZÁLEZ** con cédula de identidad 1105375842, egresado de la facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, trabajo que se encuentra bajo la dirección del Ing. John Tucker Yépez, Mg. Sc, previo a la obtención del título de Magister en Telecomunicaciones.

Es todo cuento puedo certificar en honor a la verdad, facultando al interesado en hacer uso del presente en lo que se creyera conveniente.

Atentamente,


Marco Patricio Guarnizo Cortez
LICENCIADO EN CIENCIAS DE LA EDUACIÓN MENCIÓN IDIOMA INGLES
Registro Senecyt: 1008-02-150604