UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

SEGURIDAD EN REDES 5G

TRABAJO MONOGRÁFICO
PARA OBTENER EL GRADO DE
INGENIERA EN REDES

PRESENTA
JEMIMA ELIZABET POOT POOT

SUPERVISORES
M.T.I. VLADIMIR VENIAMIN CABAÑAS VICTORIA
DR. JAVIER VÁZQUEZ CASTILLO
DR. JAIME SILVERIO ORTEGÓN AGUILAR
M.M. JOSÉ RAÚL GARCÍA SEGURA
M.S.I. LAURA YÉSICA DÁVALOS CASTILLA

CHETUMAL QUINTANA ROO, MÉXICO, JULIO DE 2022

UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

TRABAJO MONOGRÁFICO TITULADO

"SEGURIDAD EN REDES 5G"

ELABORADO POR

JEMIMA ELIZABET POOT POOT

BAJO SUPERVISIÓN DEL COMITÉ DEL PROGRAMA DE LICENCIATURA Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERA EN REDES

COMITÉ SUPERVISOR

SUPERVISOR: _____

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

SUPERVISOR: _____

DR. JAVIER VÁZQUEZ CASTILLO

SUPERVISOR: _____

DR. JAIME SILVERIO ORTEGÓN AGUILAR

SUPERVISOR SUPLENTE: _____

M.M. JOSÉ RAÚL GARCÍA SEGURA

SUPERVISORA SUPLENTE: _____

M.S.I. LAURA YESICA DÁVALOS CASTILLA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
DIVISIÓN DE CIENCIAS, INGENIERÍA Y TECNOLOGÍA

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
ÁREA DE TITULACIÓN

CHETUMAL QUINTANA ROO, MÉXICO, JULIO DE 2022

Resumen

En los últimos años, ha habido una confusión entre la definición real de 5G, pero realmente se puede definir como un conjunto de tecnologías en una sola estructura de Red que conecta personas con personas y personas con todo. La red 5G se puede clasificar como: 5G Autónomo y No Autónomo; 5G Autónomo funciona de manera individual, 5G No Autónomo es dependiente de 4G LTE.

Los principales componentes de 5G se dividen en Insumos, Infraestructura, Servicios TIC e Interfaz. Para los insumos, se considera todo lo que está relacionado con las tecnologías habilitadoras que ayudan a funcionar 5G, por ejemplo, el Espectro Electromagnético, mmWave, Pequeñas Celdas, MIMO Masivo, Formación de Haces y Estándares. En relación con Infraestructura, se cuenta con un nuevo núcleo, a comparación de 4G, llamado 5GC, nuevo nombre de Antena, gNB, RAN llamado NR, entre otros. La interfaz Xn, F1, y los Servicios TIC que ofrece como Big Data, M2M, D2D, e – Salud, Vehículos autónomos, entre otros.

La arquitectura 5G tiene diversas modificaciones por mejora, desde la división más específica entre el Plano de Control y de Usuario para admitir velocidades más avanzadas, hasta la implementación de Protocolos que mejoran la Seguridad de la Red. También, cuenta con Nuevas Bandas de Frecuencia por encima de los 6 GHz para garantizar el funcionamiento de casos de uso más avanzados y el uso paralelo de 3 distintos tipos de Frecuencias de acuerdo con el servicio que se requiere.

Este documento incluye las características que definen la exclusividad de las Redes 5G, los Riesgos que suponen como Botnets IoT y la comparación de Seguridad 4G y LTE.

Agradecimientos

A Dios, porque siempre ha estado conmigo.

A la vida, porque me ha enseñado lo maravillosa que es.

A mi abuelo, Luis Beltrán Poot Martín, que en paz descanse, por ser un gran ejemplo para mí.

A mi mejor amigo, José Luis Chi Lozano (Chilo), por ser mi fuente de inspiración, por sus consejos, amistad que me ha proporcionado en estos últimos 16 años.

A mis padres y Beau Flowers, por esos momentos.

A mis mejores amigos, Oscar Azueta Sosa, Lizzie Gabriela Briceño González, Omar Ríos Arreola, María Estela Gómez Hernández, Julio Cesar Barragán (Junior), que son unas personas increíbles, por compartir un pedacito de sus vidas conmigo, no los cambiaría por nada, a pesar de la distancia están en mi corazón.

A Doni Ever Montejo, por sus ánimos del día al día.

A mis profesores, en especial a mi querida profesora Gloria Bocarando, un gran ejemplo de persona en todos los aspectos, al profesor Rubén González Elixavide por sus regaños en su tiempo y al profesor Walter Magaña, junto con el profesor Rubén, por enseñarme la manera de explicar con pocas palabras, los admiro mucho.

A mi hija Natasha y mis compañeros.

Contenido

Tabla de Figuras

Índice de Tablas

Introducción

Las Redes de Comunicaciones Móviles han sido el sector más creciente en los últimos años y han cobrado relevancia debido a la alta demanda por parte de sus usuarios, pero conforme pasa el tiempo llegan a su límite funcional, ya que las terminales necesitan actualizarse. Es por eso, que la Telefonía Móvil está en constante crecimiento para satisfacer las necesidades de sus clientes.

5G es una tecnología de Quinta Generación para Telefonía Móvil, esencial para la transformación digital de la sociedad y el mundo. Su uso en algunos países ya se ha implementado como prueba, a mediados del 2020, el 5G tuvo un lanzamiento comercial en algunos países asiáticos y una ciudad principal de todos los estados miembros siendo un 8% de cobertura poblacional, su estandarización o recomendación UIT-R M.2083-0 se espera partir del 2021 con una cobertura poblacional del 17% (0.1 millones de conexiones 5G) y a partir del 2025 (34% de alcance poblacional) en áreas urbanas y redes de transporte.

A diferencia de otras generaciones, 5G es innovador, es el inicio de un nuevo estilo de vida muy diferente porque es parte de nuestra evolución, va más allá de lo convencional. Ofrece un sistema de costos bajos y escalables, se añaden otras funcionalidades que demandan velocidades de transmisión de datos por la red muy rápidos (rendimiento), reducción a cero el tiempo de retraso entre dispositivos y servidores (baja fluctuación de latencia y retardo), facilitando la conexión simultánea en tiempo real de hasta 100 dispositivos en cualquier lugar del mundo, suponiendo un impulso decisivo al desarrollo del Internet de las cosas (IoT), la Virtualización de la Red, donde los elementos se encuentran alojados virtualmente en servidores que gestionarán la administración de los elementos, ente otros servicios interesantes.

Todos estos beneficios traen consigo múltiples desafíos de Seguridad, como ha sucedido desde los inicios de la Telefonía, aunque el Sistema de Comunicación ha sido propensa a vulnerabilidades de Seguridad básicos, por ejemplo, en la 1G: clonación de canales inalámbricos, 2G: difusión de mensajes SPAM; con la llegada del 5G, las amenazas son más complicadas y dinámicas, por ejemplo las configuraciones erróneas de la red virtual de trabajo es un peligro inminente en general de la red ya que pone en riesgo la privacidad de los usuarios o la necesidad de un servicio más controlado y automatizado en tiempo real para su gestión.

Este trabajo presenta una investigación a nivel monografía dando relevancia a la Seguridad para Redes 5G, y así conocer el tema a mayor profundidad, ya que en estos momentos, se encuentra en mejoras de estandarización, actualización de protocolos, riesgos y soluciones para mitigar las vulnerabilidades.

Objetivo General

Identificar los diferentes aspectos de Seguridad y vulnerabilidades asociados a las Redes 5G mediante citas bibliográficas.

Objetivos Específicos

OP1.- Identificar los principales componentes de las Redes 5G.

OP2.- Describir las principales características de las Redes 5G.

OP3.- Clasificar los Riesgos de Seguridad que se presentan en las Redes 5G.

OP4.- Analizar los Riesgos de Seguridad que se presentan en las Redes 5G.

OP5.- Exponer las medidas básicas de protección para las Redes 5G.

OP6.- Comparar los aspectos de Seguridad de las Redes 5G y las tecnologías actualmente utilizadas.

Alcance

Seguridad en Redes 5G se encuentra enfocado a 5G autónomo, Telefonía Móvil de manera general y a su vez específica como caso de uso, en conjunto con IoT. Dando relevancia a las principales características de 5G, Componentes Principales, Riesgos, Análisis de los Riesgos, Métodos de Protección y Comparativa de Seguridad entre Redes 4G y 5G.

Capítulo 1: Marco de Referencia

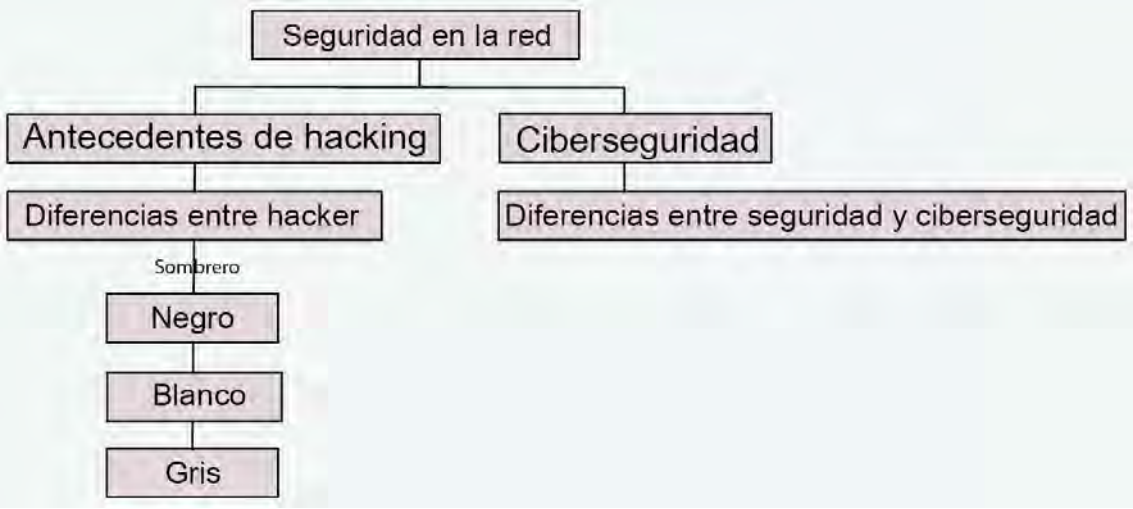


Figura 1 Organización de Seguridad. Fuente: Elaboración propia.

1.1 Seguridad en la Red

La Seguridad es esencial para las diferentes Redes de Telecomunicaciones existentes para mitigar[1] los ataques de intrusos mal intencionados, que ponen en riesgo la Integridad, Confidencialidad y la Disponibilidad de los datos[2] y dispositivos de los usuarios en distintas corporaciones. En conjunto, su funcionamiento se ayuda de Protocolos de Seguridad de la Red[3], procesos, técnicas y herramientas (ver Figura 1). [1]

[1] Disminuir.
[2] Información no alterada.
[3] Reglas de comportamiento específicos para usuarios y administradores que deben seguir dentro y fuera de la organización en determinadas situaciones.

Las organizaciones de Seguridad de Red están formadas por sociedades de profesionales en Seguridad de Red y son creadas con el propósito de establecer Políticas de Seguridad, estándares[4], inclusive subdiviendo su gestión en partes más pequeñas para que se puedan centrar en áreas precisas, estar pendientes en temas exclusivos como las vulnerabilidades de los dispositivos, amenazas nuevas, evaluando factores determinantes y poniendo en práctica las técnicas de mitigación (ver Figura 2). [1]

Figura 2 Organización de Seguridad y servicios. Fuente: Elaboración propia.

Una de las técnicas de mitigación es el desarrollo y uso de los Firewall para negar el tráfico malicioso. [1]

Tomando como referencia la definición de Cisco, “un Firewall es un dispositivo de Seguridad de la Red que monitoriza el tráfico saliente y entrante, decidiendo si debe permitir o bloquear un tráfico específico.” [2]

La empresa Digital Equipment (DEC) creó la primera generación del Firewall, inspeccionando y filtrando de manera individual cada paquete, verificando si pertenecía a las pocas reglas predefinidas en ese entonces, pero sin verificación de origen - destino. Esto favoreció que los laboratorios Bell de A&T desarrollaran Firewall Stanful, determinando si un paquete pertenece o no a un flujo existente de datos, siendo más rápido que la generación anterior. [1]

[4] Especificaciones técnicas definidas por organizaciones de estandarización.

Los Firewalls son una herramienta relevante que pueden utilizar distintos dispositivos para protegerse, hasta el día de hoy han evolucionado de manera eficiente pasando de lo básico a bloquear amenazas potenciales. [1]

El manejo de protocolos de criptografía es otro método que consiste en ocultar la información de intrusos malintencionados (ver Figura 3). Este dispone de algoritmos de encriptación antes de ser enviado, por ejemplo, encriptación simétrico si se envía un mensaje que utiliza números y letras, realiza una combinación de caracteres distintos (Hash) haciendo que la información no se entienda, esto trae consigo muchos beneficios como una buena Confidencialidad de los datos, es decir, que sólo el receptor con ayuda de un algoritmo de desencriptación, la llave para desbloquearlo, puede leer el contenido, la Disponibilidad de contar con la información cuando se requiera mientras llegue y la Integridad de los datos al no ser alterados por terceras personas, el mensaje llega tal cual se envió sin ninguna modificación. [1]

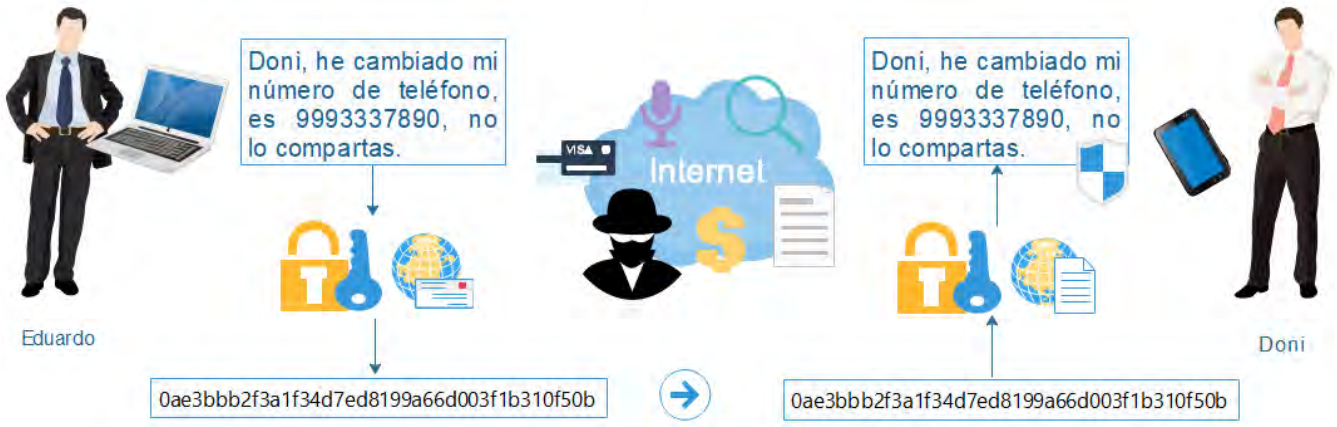


Figura 3 Envío de mensaje utilizando encriptación. Fuente: CCNA Security. [1]

1.1.1 Definición de Seguridad

La Seguridad en la Red involucra seguridad de la información de datos que se encuentra dentro de la red. “Abarca las medidas y las actividades que intentan proteger los activos de información, es decir, la protección de la información o datos que tienen valor para una organización a través de la reducción de riesgos y mitigando las amenazas posibles. Estos activos pueden utilizarse en diferentes formatos, por ejemplo de manera digital, física o en forma de ideas o conocimientos de personas que pertenecen a la organización.” [3]

Mantener una red segura a través de estrategias formales garantiza la seguridad de los usuarios de la red, ofreciendo Estabilidad y Confidencialidad, previniendo de manera oportuna los efectos negativos a mediano o largo plazo. [1]

1.2 Hacking

1.2.1 Antecedentes del Hacking

En los inicios del Internet, de momento no se tomaba en cuenta las vulnerabilidades existentes porque los usuarios realizaban prácticas elementales como la investigación y el desarrollo, era un ambiente seguro sin preocupaciones, no existían intensiones de afectar a otros usuarios para obtener un bien. [1]

En la década de los 50´s, un club de ferrocarrileros recibió una donación de teléfonos usados, logrando construir un sistema complejo que permitía marcar las rutas que llevaría a los ferrocarriles hacia un determinado lugar, a ese nuevo uso que les dieron a los equipos telefónicos les llamaron “hackear” y a las personas que elaboraron el sistema se conocieron como: “los hackers originales”. Posteriormente, pasaron a la programación en tarjetas perforadas y cintas de teletipo para las primeras computadoras como la TX Cero. [4]

La experiencia adquirida en ese proyecto facilitó que dentro del grupo, se especializaran de manera individual en distintas áreas según sus intereses; por ejemplo parte de los integrantes estaban interesados con programas de escritura, otros en la búsqueda creativa para utilizar menos tarjetas perforadas dentro del programa, es decir, no usar tantos recursos para el mismo objetivo; una minoría adoptó una cultura subinformal, con el interés de aprender, querían tener al alcance la información de manera gratuita a toda costa por diversos motivos, ya sea para estar al mismo nivel académico de la burocracia de las clases universitarias, la discriminación, falto de recursos económicos, lograron desafiar lo convencional transcendiendo. [4] Un claro ejemplo se dio en la década de los 60´s y 70´s, en Universidades como Berkeley CalTech Stanford, los alumnos con la aparición de la tecnología, un Centro de Cómputo, la mayoría querían experimentar con los equipos, aprender de ellos de manera práctica, pero no sabían cómo comenzar. [6]

1.2.2 Definición de Hacking

Hacking en la mayoría de los casos hace referencia a infringir la ley, realizar actos vandálicos, descargar información sensible personal, empresarial que ponen en riesgo empresas prexistentes, la Seguridad de las personas o su economía, para otros también asiduamente son profesionales de Red que utilizan sus habilidades de programación sofisticada de Internet, para garantizar que las Redes no están expuestas a los ataques. En realidad, se dividen en varios grupos dependiendo sus acciones, pero todos evolucionan, resuelven problemas de manera creativa, buscando infinidad de soluciones de Seguridad distintas a lo convencional, impulsando la Seguridad. [1]

1.2.3 Diferencias entre Hacker

Dependiendo de sus acciones, se dividen en: Hacker de Sombrero Blanco, Hacker de Sombrero Negro o Gris.

1.2.3.1 Hacker de Sombrero Blanco

También llamado Hacker Ético.

Un Hacker Ético es un profesional en Seguridad de Red que utiliza todos sus conocimientos adquiridos de Seguridad, Políticas, estándares, de acuerdo con las leyes para verificar las vulnerabilidades de la Red con permiso del propietario, dispone herramientas y técnicas avanzadas que un atacante utilizaría. Muchas empresas contratan a un Hacker Ético para realizar simulaciones de manera segura, verificando la eficacia de sus sistemas de Seguridad, desarrollando estrategias que se puedan perfeccionar de acuerdo con los resultados obtenidos. Las simulaciones se realizan mediante un Software de escaneo para verificar los puertos y servicios en un rango de direcciones IP. Se da como resultado una lista de riesgos a cubrir o como un intruso podría ingresar en el medio y perder el control de los Sistemas. [5]

Contar con buenas herramientas de Seguridad evitan tener una falsa sensación de Seguridad o fallar en la búsqueda de amenazas, asimismo es importante actualizar constantemente sus habilidades para estar al corriente de las últimas amenazas. [5]

1.2.3.2 Hacker de Sombrero Negro

Según Allen Harper (2018) son actores maliciosos que tienen una variedad de motivaciones y tácticas, la escala y complejidad de sus ataques está en aumento. [5]

Su motivación se puede basar en la política robando secretos de estado, en la economía realizando fraudes bancarios o simplemente generar enormes ganancias de dinero de manera fácil, causas sociales o por venganza personal, comprometen la estabilidad de la Red y en la mayoría de los casos son difíciles de detectar pasando desapercibidos, sólo en algunos casos se anuncian, atacan los servidores y vuelve inutilizable los servicios. [5]

1.2.3.3 Hacker de Sombrero Gris

Es una combinación de ambas.

1.3 Ciber

"Ciber puede consistir en muchos componentes familiares de nuestra vida diaria como Internet, Telefonía Móvil y fija, entre otros temas relacionados con la Informática y la conectividad a Redes de Datos internas y externas. Además del entorno, ya que somos capaces de observarlo, cibernético también tiene que ver con los secretos ocultos, la protección y las intenciones de ataques para robarlos y exponerlos." [18]

1.3.1 Ciberataque o Amenazas Cibernéticas

Podemos determinar que una amenaza cibernética como "eventos o explotación deliberada de vulnerabilidades por agentes de amenazas o vectores de ataque que conducen la interrupción de las operaciones, pérdida o control de los activos de una organización." [20]

"Un amplio espectro de tipos de ataques cibernéticos podría incluir la intrusión, vigilancia, registro de datos, espionaje, extracción, destrucción y manipulación de datos, robo de la propiedad intelectual, control de dispositivos, propiedad e infraestructura crítica, efecto letal individual y operaciones con el impacto nacional. La ciberseguridad proporciona las contramedidas para los Ciberataques." [18]

1.3.1.1 Componentes de Ciberataques

"En general, los Ciberataques se pueden clasificar en tres componentes;

1.3.1.1.1 Inteligencia

Para obtener acceso, ejecutar la carga útil cibernética, comprender el entorno del objetivo.

1.3.1.1.2 Armas

Específicas del objetivo y activadas en condiciones especialmente planificadas.

1.3.1.1.3 Decisión humana calculada

La combinación de éstas forma una fuerza cibernética." [18]

1.3.1.2 Tipos de Ciberataques

Estos se clasifican en cinco niveles:

1.3.1.2.1 Ciberactivismo

"Es el primer nivel de amenaza e implica ciber vandalismo. La intención de los actores es no causar ningún daño, ya que puede estar utilizado el ataque para avergonzar una organización o enviar un mensaje político.

Los hacktivistas son personas o grupos que "realizan hack" los sitios web disponibles públicamente y sobrecargan los servidores de correo electrónico para enviar un mensaje de motivación política o utilizarlo para transmitir un mensaje de protesta, por ejemplo, contra la limitación de las libertades civiles." [20]

1.3.1.2.2 Ciberdelito

“Implica el uso de Redes y Sistemas de Información por parte de los adversarios para la comisión de un delito contra la infraestructura de IT de la víctima. Este acto puede ser perpetuado por individuos, grupos poco organizados, terroristas, personas con información privilegiada o spammers. El motivo de tal ataque puede ser Fraude y falsificación.” [20]

1.3.1.2.3 Ciberespionaje

“Es el uso de los medios ilegales en Internet, Redes de Telecomunicaciones, programas, computadoras, para obtener información secreta de individuos, organizaciones, competidores y gobiernos con fines políticos, militares o monetarios. Es realizado por agentes de inteligencia, profesionales, individuos o grupos que explotan las vulnerabilidades en el sistema del adversario para obtener información de alto valor.” [20]

1.3.1.2.4 Ciberterrorismo

“Ciberataques dirigidos a los sistemas informáticos o la infraestructura crítica de organizaciones gubernamentales y privadas, con la intención de intimidar al gobierno o causar pánico entre la población civil. Es perpetuado por sofisticados grupos terroristas cuyo objetivo es captar la atención nacional e internacional. Utilizan armamento informático ofensivo, ya sea de forma aislada o una combinación con otros medios de ataque.” [20]

1.3.1.2.5 Guerra Cibernética

“Implica la conducción de guerra en el mundo virtual o en el ciberespacio. Los agentes de amenazas típicos son las fuerzas armadas y los servicios de inteligencia de los estados nacionales, los grupos insurgentes organizados o los terroristas. La acción tiene como objetivo inmovilizar el sistema de información o destruir la infraestructura crítica del enemigo mediante el uso de armas como virus informáticos, gusanos o ataques de denegación de servicio (DOS).” [20]

“Ciberguerra es llamado a una operación cibernética desde el punto de vista militar. Uno de los puntos clave de la guerra cibernética es que puede causar lesiones o la muerte de personas, daños o destrucción de objetos.” [18]

Estos conceptos de los diferentes tipos de ciber amenazas se han categorizado por niveles según su gravedad, este puede venir de cualquier lado y con una combinación de actores a la vez. [20]

Algunos ejemplos de Ciberataques son DoS, DDoS, MITM, Spamming, Phishing, Explotación del Día Cero, entre otros. [18]

1.3.1.3 El costo de los Ciberataques

El costo real de los ataques es difícil de cuantificar, pero se estima por ejemplo en EE. UU. oscilan entre 24 mil millones de dólares y 120 mil millones de dólares, el costo a nivel mundial se ha reportado hasta 1 billón de dólares, la propiedad intelectual en Estados Unidos pierde aproximadamente 300 mil millones de dólares mensuales. Solamente enfocado en el ciberdelito según Ponemon Institute descubrió que el costo era alrededor de 15 millones de dólares para las organizaciones, aumentando el 19% en la cifra de una encuesta del 2014. [20]

El costo relacionado con los Ciberataques se puede dividir en dos costos:

1.3.1.3.1 El costo preventivo

Es invertir en una organización para prevenir una intrusión o reducir el impacto que pueda tener. Aunque el costo de las soluciones preventivas puede ser alto, es posible que no sea tan costoso como los remedios posteriores a los ataques. [20]

1.3.1.3.2 El costo posterior al ataque

Implica el costo real como la cantidad robada o extorsión. Incluyendo el costo de reemplazo, rescate, reparación de la infraestructura, reconstrucción de imagen, costo de detención, notificación [20]

1.3.1.4 Consecuencias de Ciberataque

"En cuanto a la vista humano, hay dos tipos de consecuencias de Ciberataque:

Las no violentas pero impactantes para las funciones de la sociedad de la información, como puede ser la llamada destrucción y disrupción virtual, que conducen a daños físicos y destrucción. [18]

Un ejemplo clásico de ciberataque fue en el 2010, el virus Stuxnet infectó grandes Unidades de Control de centrifugadoras nucleares específicas, lo que provocó que aceleraran y se autodestruyeran. Este caso es una prueba concreta de magnitud de las consecuencias que puedan acarrear los posibles ataques. Además del daño físico, también pueden resultar en una destrucción total y permanente del almacenamiento de información. [18]

1.3.2 Seguridad Cibernética

"La Ciberseguridad está enfocado a la protección de la información digital de los sistemas. Por ello se puede considerar que la Ciberseguridad está comprendida dentro de la Seguridad de la información." [3]

Según Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) "La Seguridad Cibernética generalmente la brindan proveedores externos específicos como un servicio, un producto o una combinación de producto y servicio, que ayudan a las organizaciones y a las personas a proteger sus activos digitales." [20]. "Hay dos tipos distintos de organización cuyo negocio depende de la Seguridad: las organizaciones que están directa o indirectamente involucradas con la entrega de soluciones de Seguridad, vendiéndola como un servicio o paquete y aquellas que se enfrentan a las amenazas potenciales de los Ciberataques." [20]

1.3.2.1 Servicios de Seguridad en Redes Inalámbricas

- Autenticación
    - Entidad
    - Mensaje
- Confidencialidad

    - Datos
    - Privacidad
- Disponibilidad
- Integridad
- Otros: no repudio, Imputabilidad y Autorización. [31][41]

1.4 Diferencia entre Seguridad en la Red y Ciberseguridad

A pesar de que Seguridad de la Red y Ciberseguridad tengan conceptos similares, existe mucha diferencia entre las funciones reales entre ambos.

“Los Ciberataques son una realidad y su papel será muy importante en los próximos años con la evolución de 5G e IoT juntos. No sólo tendrán un impacto en el rol de fuerzas de defensa, sino también en nuestra vida diaria.” [18] Ciberseguridad aplica para Ciudades Inteligentes donde se utiliza un conjunto de componentes o servicios, incluido Telefonía Móvil en sistemas donde circula la información a proteger. [3]

En cambio, Seguridad “tiene un alcance mayor que la ciberseguridad ya que poner Seguridad de la información involucra protegerla en todos los estados o formas de los diferentes riesgos a las que se enfrentan… instintivamente si se encuentran interconectados o no. Se sustenta en metodologías, normas, técnicas, herramientas tecnología entre otros elementos que soportan la idea de protección en las distintas facetas de información.” [1][3]

1.5 Telefonía Móvil

1.5.1 Definición de Sistema Celular

"Es una colección de entidades que consta de tres elementos básicos: la Estación Móvil[5], la Estación Base[6] (BS) y el Centro de Conmutación Móvil (MSC)[7]." [9]

N número de Estaciones Móviles dentro del rango permitido a través de una Interfaz de Radio[8] se comunican con una Estación Base, cada Estación Base está conectado al Centro de Conmutación Móvil a través de Sistemas de Transmisión de Línea Fija. Las Estaciones Móviles deben estar dentro del Patrón de Radiación[9] que emite la BS para establecer una conexión, ya que todas las comunicaciones siempre deben pasar por la Estación Base y el Conmutador. [9]

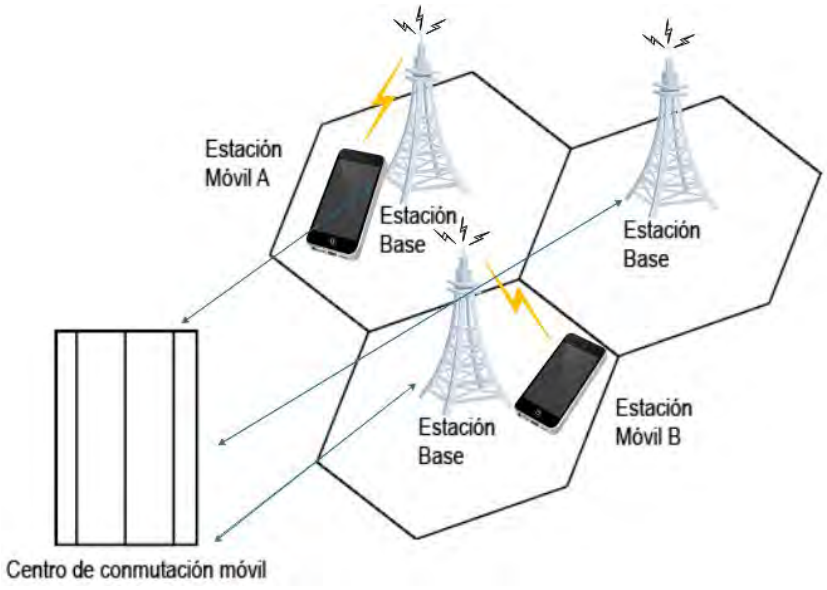


Figura 4 Arquitectura genérica de un Sistema Celular. Fuente: Yu-Kwong (2007) [9]

(Ver la Figura 4 y 5), la Estación Móvil A y la Estación Móvil B directamente no se pueden comunicar, por qué necesita de una BS y el Centro de Conmutación Móvil que son los

[5] Teléfono Móvil.
[6] Antena que administra la señal. Se extiende por la tierra [14] por medio de fibra óptica.
[7] Central donde se conmutan las llamadas, estableciendo rutas punto a punto entre el transmisor (Tx) y receptor (Rx). (MSC)
[8] Interfaz entre el Equipo del Usuario y la Estación Base.
[9] Representación gráfica de las propiedades de radiación de una Antena.

intermediarios. También se necesita de la Fuente, la voz qué es el mensaje de entrada en forma de señal analógica.[10]

El micrófono del Teléfono Móvil traduce la señal analógica en señal eléctrica[11] porque no se puede transmitir, el transductor[12] lee la onda[13] de la señal eléctrica y lo traduce a lenguaje máquina, en unos y ceros, enviando la señal a la Estación Base siendo este el transmisor[14], la Estación Base sabe dónde transmitir la señal, al tener que ser interceptado por el receptor[15] con ayuda del Centro de Conmutación Móvil ya definido, la señal generada viaja través del Canal de Comunicaciones utilizando una Banda de Frecuencias, pero la Capacidad del Canal[16] disminuye por diversos obstáculos por ejemplo el Ruido Térmico causado por la temperatura del ambiente o el Ancho de Banda por medio de la Distorsión, Interferencia, Refracción, Difracción, la Absorción Atmosférica, entre otros.

Para que exista una comunicación eficiente, es necesario mitigar el elemento que hace que la capacidad del canal disminuya y señal de voz en forma de onda no se vea afectado, o bien si el obstáculo es la Absorción Atmosférica donde las señales se pierden por la curvatura de la tierra, una solución es instalar suficientes Estaciones Bases que ayuden a captar la señal y dirigirlo al receptor.

De esta manera, el transductor al leer la onda de la señal digital la convierte en señal analógica, donde la Estación Móvil B recibe el mensaje. [10] *Para más información examine tema "Efectos de propagación de Radio Celular" página 16.*

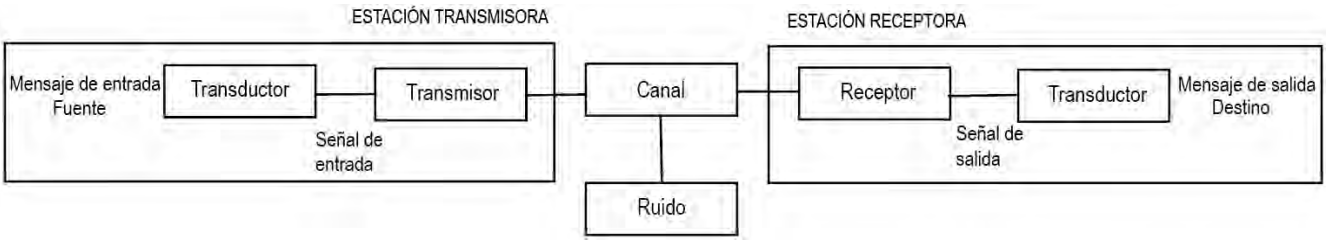


Figura 5 Elementos que comprenden un Sistema de Comunicación. Fuente: Ibarra, Raul (2007) [23]

[10] Se encuentra en el ambiente, varia con el tiempo, a mayor distancia, mayor degradación.
[11] Se genera por un fenómeno electromagnético.
[12] Convierte energía en señal digital o viceversa.
[13] Propagación de energía de una propiedad en un medio.
[14] Transmite, envía la señal hacia el receptor destino.
[15] Recibe la señal que envía el transmisor origen.
[16] "Velocidad de datos máxima alcanzable." [32]

1.5.2 Banda de Frecuencias

La señal que viaja por el Canal de Comunicaciones desde el transmisor hasta el receptor, con ayuda del MSC, utiliza una Banda de Frecuencias.

Según Adipta Gupta (2019) “Frecuencia simplemente significa la frecuencia que ocurre un evento. En el caso de Radio, significa el número de ciclos de una onda, por cada segundo dado o tasa de oscilación de ondas.” [8] La Frecuencia es el número de veces de movimientos repetidos que frecuentemente se forma en una señal.

“El Espectro Electromagnético es el rango de todos los tipos de radiación electromagnética que incluye ondas de Radio a rayos gama,”[14] es decir, es el conjunto o rango de todas las Frecuencias que produce una radiación electromagnética.

Existen diferentes Bandas de Frecuencias basados en rango de Frecuencias (véase Tabla 1). [8]

Tabla 1 Diferentes Bandas de Frecuencia y su clasificación. Fuente: Aditya Gupta (2019)[8]

Clase	Abreviación	Rango de frecuencias
Extremely Low Frecuency	ELF	< 3 kHz
Very Low Frecuency	VLF	3 – 30 kHz
Low Frecuency	LF	30 – 300 kHz
Medium Frecuency	MF	300 – 3000 kHz
High Frecuency	HF	3- 30 MHz
Very High Frecuency	VHF	30 – 300 MHz
Ultra Hight Frecuency	UHF	300 – 3000 MHz
Super High Frecuency	SHF	3 – 30 GHz
Extremely High Frecuency	EHF	30 – 300 GHz

La comunicación móvil depende del espectro radioeléctrico para realizar sus funciones.” [14] “El término espectro de Radio se refiere al rango de Frecuencias de 3 MHz a 300 kHz correspondientes a longitudes de onda que varían de 100 km a 1mm. El intercambio de

información se lleva a cabo variando la Amplitud, Fase y Frecuencia de las ondas de Radio portadora[17].” [14]

(Ver Figura 6), las asignaciones de la Banda de Frecuencia exclusivas para los servicios móviles y fijos a nivel general.

Asignación para servicios móviles y fijos

Frecuencia	Región 1	Región 2	Región 3
410–430 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
440–470 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
470–890 MHz	790–862 FIJO, MÓVIL	698–806 MÓVIL	FIJO, MÓVIL
	862–890 FIJO, MÓVIL	806–890 FIJO, MÓVIL	
890–960 MHz	890–960	890–902 FIJO, MÓVIL	890–960
		902–928 FIJO	
		928–960 FIJO, MÓVIL	
1427-1525 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
1525-1530 MHz	REPARADO	-	REPARADO
1668,4–1690 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
1700-1710 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
1710-2170 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
2170-2520 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
2520–2690 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
2700–4800 MHz	3400–4200 FIJO	3400–3500 FIJO	3400–3500 FIJO
	4400–4800 FIJO, MÓVIL	3500–4200 FIJO, MÓVIL	3500–4200 FIJO, MÓVIL
		4400–4800 FIJO, MÓVIL	4400–4800 FIJO, MÓVIL
4800–5000 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
5150–5350 MHz	MÓVIL	MÓVIL	MÓVIL
5470–5725 MHz	MÓVIL	MÓVIL	MÓVIL
5850–8500 MHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
10–10,45 GHz	FIJO, MÓVIL	-	FIJO, MÓVIL
10,5-10,68 GHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
10,7-11,7 GHz	FIJO, MÓVIL	FIJO, MÓVIL	FIJO, MÓVIL
11,7–14 GHz	11,7-12,5 FIJO, MÓVIL	11.7–12.1 FIJO	11.7-13.25 FIJO, MÓVIL
	12,75-13,25 FIJO, MÓVIL	12.2-13.25 FIJO, MÓVIL	
14–15,4 GHz	14.3–14.4 FIJO, MÓVIL	14.4-15.35 FIJO, MÓVIL	14.3–14.4 FIJO, MÓVIL
	14.4-15.35 FIJO, MÓVIL		14.4-15.35 FIJO, MÓVIL
15,4–18,4 GHz	17.7-18.1 FIJO, MÓVIL	17,7-17,8 FIJO	17.7-18.1 FIJO, MÓVIL
	18.1-18.4 FIJO, MÓVIL	17.8-18.1 FIJO, MÓVIL	18.1-18.4 FIJO, MÓVIL
		18.1-18.4 FIJO, MÓVIL	
18,4–22 GHz	18.4-19.7 FIJO, MÓVIL	18.4-19.7 FIJO, MÓVIL	18.4-19.7 FIJO, MÓVIL
	21.2-22 FIJO, MÓVIL	21.2-22 FIJO, MÓVIL	21.2-22 FIJO, MÓVIL
22-24,75 GHz	22–23,6 FIJO, MÓVIL	22–23,6 FIJO, MÓVIL	22–23,6 FIJO, MÓVIL
	24.25-24.75 FIJO		24.25-24.75 FIJO, MÓVIL
24,75–29,9 GHz	24,75-25,25 FIJO	-	24,75-25,25 FIJO
	25.25–29.5 FIJO, MÓVIL 31–	25.25–29.5 FIJO, MÓVIL 31–	25.25–29.5 FIJO, MÓVIL 31–
29,9–34,2 GHz	31.3 FIJO, MÓVIL	31.3 FIJO, MÓVIL	31.3 FIJO, MÓVIL
	31,8–33,4 FIJOS	31,8–33,4 FIJOS	31,8–33,4 FIJOS
34,2–40 GHz	36–40 FIJO, MÓVIL	36–40 FIJO, MÓVIL	36–40 FIJO, MÓVIL
40–43,5 GHz	40–40,5 FIJO, MÓVIL	40–40,5 FIJO, MÓVIL	40–40,5 FIJO, MÓVIL
	40,5–43,5 FIJO	40,5–43,5 FIJO	40,5–43,5 FIJO
71–76 GHz	71–76 FIJO, MÓVIL	71–76 FIJO, MÓVIL	71–76 FIJO, MÓVIL
81–86 GHz	81–86 FIJO, MÓVIL	81–86 FIJO, MÓVIL	81–86 FIJO, MÓVIL

Figura 6 Asignación de Bandas de Frecuencias para servicios móviles y fijos. Fuente: Saad Z. Asif (2019) [14]

[17] Traslada el espectro radioeléctrico para transmitir.

1.5.3 Reutilización de Frecuencias

"Es el proceso en el cual se puede asignar el mismo conjunto de Frecuencias (canales) a más de una Célula, siempre estén alejadas a cierta distancia," [13] llamado grupo.

Sin embargo, "A las Celdas adyacentes se les asignan diferentes Frecuencias para evitar interferencias." [11]

1.5.4 Definición Radio Celular

"Es una técnica que se desarrolló para aumentar la capacidad disponible para el servicio de radiotelefonía móvil." [11]

1.5.5 Organización Celular

Es importante destacar que instalar suficientes Estaciones Base ayuda amplificar y captar la señal de manera precisa, ya que el alcance[18] de este elemento es muy pequeño, sólo puede ser utilizado por n número de Estaciones Móviles que se encuentran dentro del rango permitido que es el Patrón de Radiación que emite la Antena[19]. El Patrón de Radiación que emite la Estación Base al ser pequeña se llama Celda o Célula. Cada Celda tiene su propia Estación Base y una Banda de Frecuencias.

Cada Célula se define por el número de Estaciones Móviles permitidas, tiene forma hexagonal brindando una cobertura total del área. Un conjunto de Células forma un panal llamado Macrocélulas, en un área geográfico por ejemplo en un país pueden existir diferentes números de estas, en una ciudad solamente un conjunto de Células. [13]

[18] Disponibilidad.
[19] "Es el componente responsable de convertir la información en señales electromagnéticas que pueden viajar a través del medio de propagación (generalmente aire)." [8]

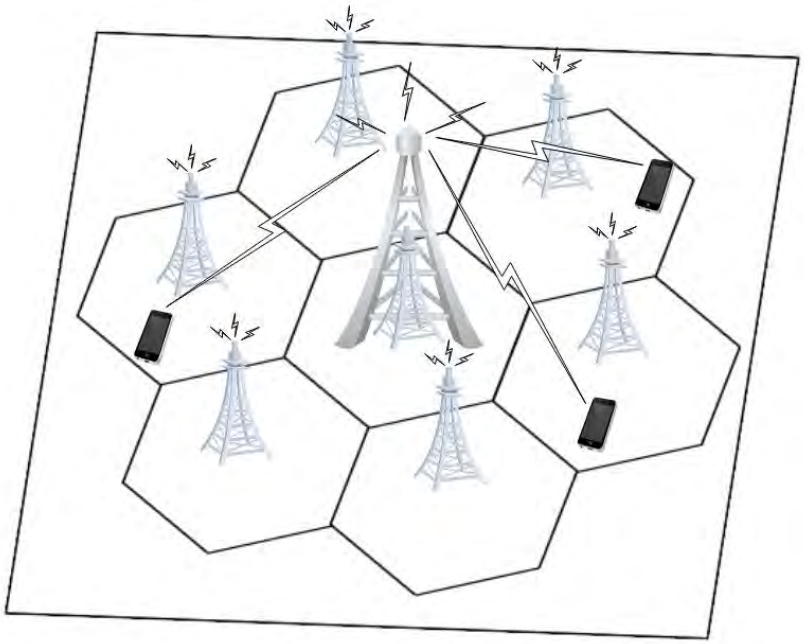


Figura 7 Macrocélulas durante la etapa de implementación de una Red Celular. Fuente: Yu-Kwong (2007) [9]

(Examine la Figura 7), la formación de una Macrocélula como un conjunto de Células, cada Célula con una BS y (la Figura 8) la representación de una Macrocélula en una ciudad.

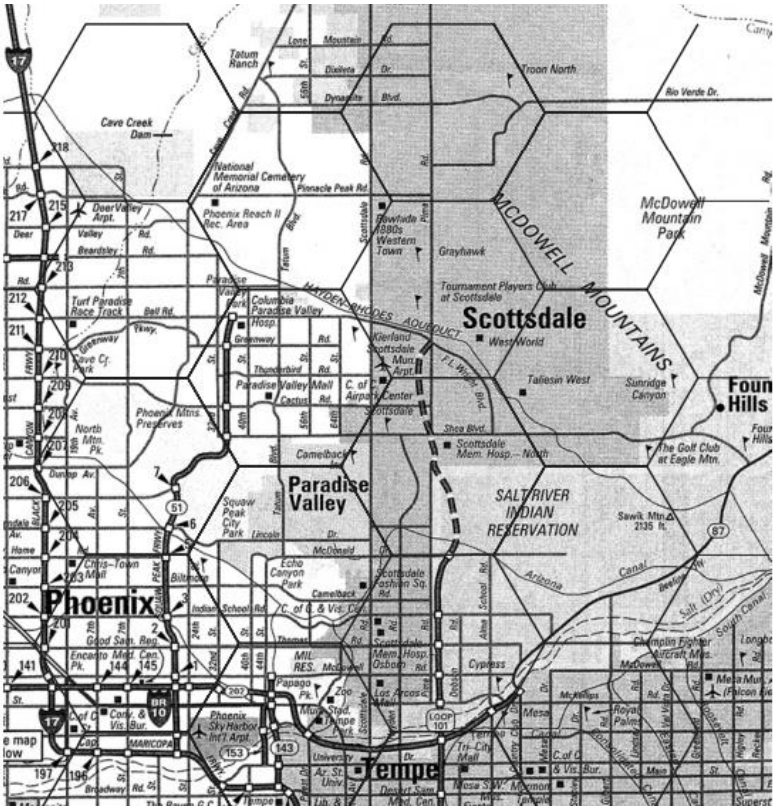


Figura 8 Retícula de Células hexagonales sobrepuesta en un área metropolitana. Fuente: Wayne Tomasi (2003) [13]

Las Células se pueden dividir en partes más pequeñas para incrementar la capacidad de rendimiento de las Macrocélulas. [17]

Una Célula pequeña Según Small Cell Forum “es un término genérico para los nodos de Radio de baja potencia que operan en espectro con licencia y sin licencia que tienen un alcance de 10 m a varios cien. El término incluye Femtocélula, Picocélula, Microcélula.” [14] De acuerdo con las divisiones de Células o subdivisiones.

“Una Femtocélula es una Estación Base autónoma de corto alcance y bajo consumo. Una Picocélula es una Estación Base compacta de baja potencia que se utiliza en áreas públicas interiores, una Microcélula es una Estación Base de corto alcance dirigida para mejorar la cobertura para los usuarios de interiores o exteriores donde la cobertura macro es insuficiente. Si las Células pequeñas y Macrocélulas tradicionales se implementan en una Red, forman juntas una HelNet o Red Heterogénea.” [14]

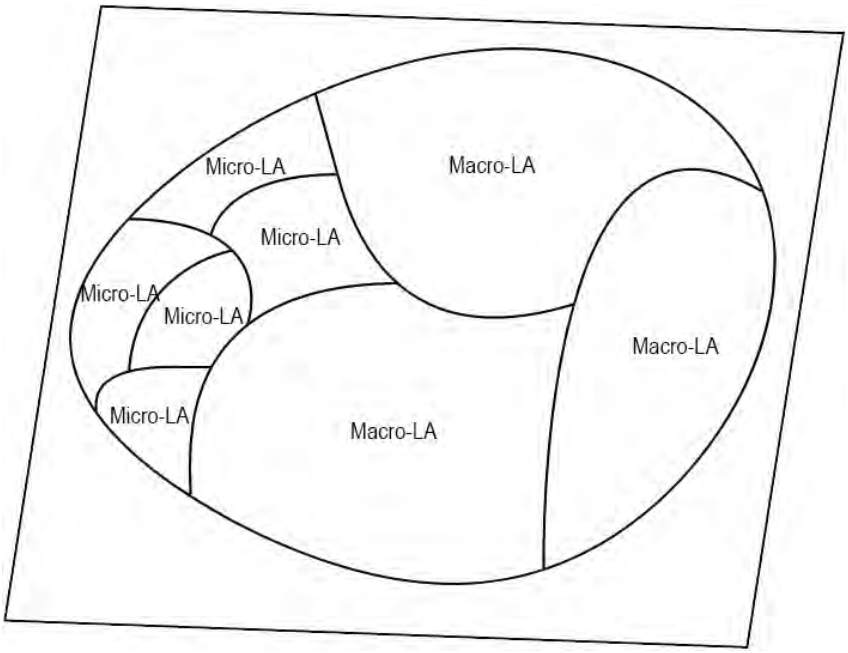


Figura 9 Helnet. Fuente: Yu-Kwong (2007) [9]

(Véase la Figura 8), una agrupación entre micro y Macrocélulas en una misma estructura. [9]

1.5.6 Elementos de una Red Celular

En la siguiente Tabla podemos ver los elementos principales de un Sistema Celular. (*Puede apoyarse de la Figura 4).*

Tabla 2 Elementos de una Red Celular. Fuente: Elaboración propia, basado en [11] [13]

Elemento de una red principal	Descripción
Centro Electrónico de Conmutación	Es la central principal donde se conmuta las llamadas y el procesamiento de los datos recibidos de los controladores del sitio. Contiene información de la SIM[20] del usuario. [13]
Controlador de Sitio	"Administra cada Canal de Radio en cada sitio, supervisa llamadas, enciende y apaga el radiotransmisor[21] y receptor[22]… hace pruebas de diagnóstico al equipo del sitio". [13]
Radio Transceptores	Es un dispositivo que envía o recibe señales sintonizado a la misma frecuencia. Por ejemplo: • FM[23] para banda angosta. • QPSK[24] para sistemas digitales. [13]
Interconexiones del Sistema	Conexión entre estaciones o MSC.
Unidades Telefónicas Móviles y Portátiles	Estación Móvil, en este caso.
Protocolo de Comunicación	Reglas que determinan como será la llamada.

1.5.7 Pasos de una llamada típica entre usuarios móviles

La señalización se puede dar entre canales y estaciones móviles, MSC públicas y privadas, estaciones y combinadas entre sí dependiendo el procedimiento.

[20] "Tarjeta inteligente desmontable… se utiliza para probar la identidad del usuario con el operador." [12]
[21] Señal de Radio transmitida
[22] Señal de Radio recibida
[23] Frecuencia Modulada
[24] Tipo de modulación

Tabla 3 Pasos de una llamada entre dos usuarios. Fuente: Elaboración propia, basado en Stallings William (2007) [11]

Procedimiento	Descripción
Iniciación de la Estación Base	1. "Cuando el móvil está encendido, escanea y selecciona el canal de configuración más fuerte," [11] es decir, el más cercano y lo monitorea. 2. "Automáticamente selecciona la Antena de la Celda en la cual operará." [11] Se produce un enlace entre la Estación Móvil y la BS. "Este procedimiento de exploración se repite periódicamente" [11] debido a la movilidad[25] del usuario mientras realiza la llamada, si sale del rango del Patrón de Radiación automáticamente se selecciona una nueva Estación Base próximo para no perder la señal. (*Ver Figura 10)*
Llamada originada en una Estación Móvil	El usuario al realizar una llamada, solicita la conexión a través de la BS y el MSC enviando la información necesaria, para llegar a la Estación Móvil destino. [11] *(Ver Figura 11)*
Paginación	"El MSC envía un mensaje de búsqueda a ciertas BS según el número de móvil llamado. Cada BS transmite la señal de búsqueda en su propio Canal de configuración asignado." [11] *(Ver Figura 12)*
Llamada aceptada	Cuando una BS encuentra la Estación Móvil de búsqueda dentro de su Celda establece una petición de llamada, y el receptor al aceptar la llamada "las dos unidades móviles sintonizan en el mismo canal designado." [11] *(Ver Figura 13)*
Llamada en curso	"Mientras se mantiene la conexión, las dos unidades móviles intercambian señales de voz y datos, pasando por sus perspectivas BS y MSC." [11] *(Ver Figura 14)*
Terminación de la llamada	"Cuando uno de los dos usuarios cuelga, se le informa al MSC y se liberan los canales de tráfico en las dos BS." [11]

[25] Velocidad máxima de la Estación Móvil cumpliendo la Calidad de Servicio (QoS) mínimo. [8]

En las Figuras siguientes podemos observar las diferentes etapas de una llamada entre dos usuarios.

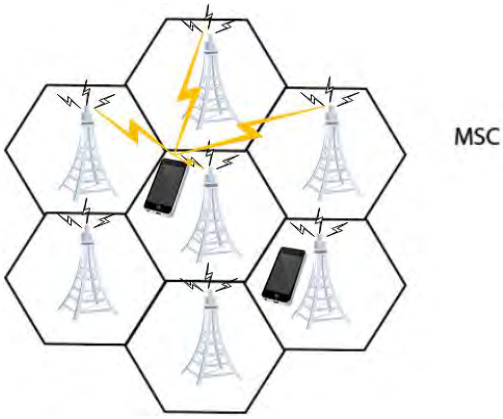


Figura 10 Monitoreando la señal más fuerte. Fuente: Stallings William (2007) [11]

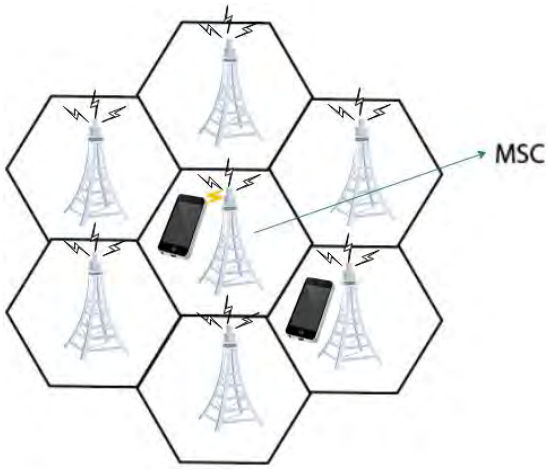


Figura 11 Solicitud de conexión. Fuente: Stallings William (2007) [11]

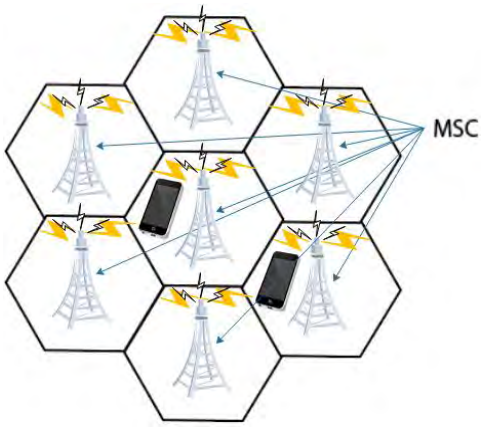


Figura 12 Paginación. Fuente: Stallings William (2007) [11]

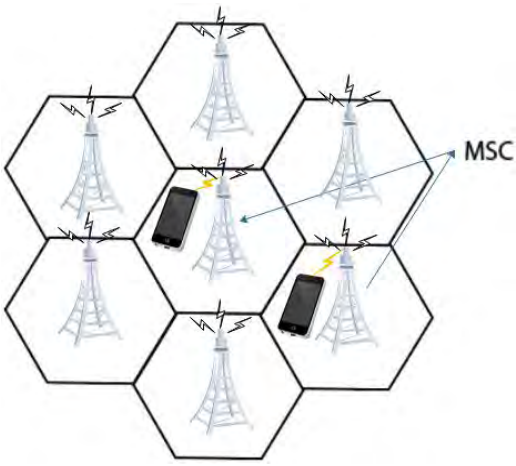


Figura 13 Llamada aceptada. Fuente: Stallings William (2007) [11]

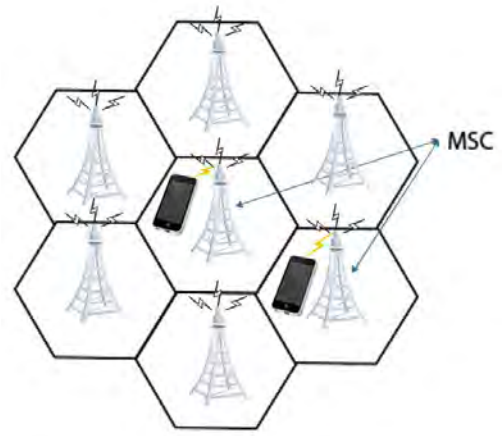


Figura 14 Llamada en curso. Fuente: Stallings William (2007) [11]

Tabla 4 Otras funciones en la comunicación entre dos usuarios. Fuente: Elaboración propia, basado en Stallings William (2007) [11]

Otras funciones	Descripción
Bloqueo de llamadas	Si el MSC al enviar un mensaje de búsqueda a ciertas BS en la etapa de paginación y estas se encuentran ocupados, "entonces la Estación Móvil realiza un número preconfigurado de intentos repetidos. Después de un número de intentos fallidos, se devuelve al usuario con un tono de ocupado." [11]
Caída de llamada	A mayor distancia, mayor degradación de la señal, eso quiere decir, que cuando una Estación Móvil sale de una Macrocelda, la señal se atenúa[26].

1.5.8 Efectos de propagación de Radio Móvil

La señal a medida que pasa por el canal de comunicaciones sufre cambios que se incorporan en la transmisión.

Algunos de esos cambios son los siguientes:

1.5.8.1 Intensidad de la señal

Es la potencia de la señal apta requerida para transmitir entre la BS y la Estación Móvil, clasificándose como la ideal, si la potencia de la señal es mayor que lo necesario, crea interferencia entre otras Celdas, dependiendo cuánto sobrepasa el límite necesario. Asimismo la intensidad de la señal depende de la posición de la Estación Móvil o su movilidad. [11]

1.5.8.2 Desvanecimiento

Según William Stallings (2007) el desvanecimiento se refiere a "la variación en el tiempo de la potencia de la señal recibida causada por cambios en el medio de transmisión."

[26] Propiedad de la energía de la señal cuando pierde intensidad mientras se aleja de una antena.

La pérdida inclusive puede generarse si la Estación Móvil se encuentra dentro del área que abarca la señal de la Estación Base, debido a cofactores que pueden interferir con la señal y debilitarla provocando errores.

Algunos tipos de desvanecimiento son:

1.5.8.2.1 Tipos de desvanecimiento

1.5.8.2.1.1 Plano

"Es el tipo de desvanecimiento en el que todos los componentes de frecuencia de la señal recibida fluctúan en las mismas proporciones simultáneamente." [11]

1.5.8.2.1.2 Selectivo

"Si la atenuación se produce en una parte del Ancho de Banda de la señal." [11]

1.5.8.2.1.3 No selectivo

"Implica que el Ancho de Banda de la señal de interés es más estrecho y está completamente cubierto por el espectro afectado por el desvanecimiento." [11]

1.5.9 Propagación de trayectos múltiples

Entre los tipos de propagación de la señal tenemos:

1.5.9.1 Reflexión

Según Stallings Williams (2007) "La señal electromagnética encuentra una superficie que es grande en relación con la longitud de onda de la señal." [11]

Por su parte, Wayne Tomasi (2003) "Reflejar quiere decir regresar, y la reflexión es el acto de reflejar. La reflexión electromagnética se presenta cuando una onda incidente choca con una

frontera entre dos medios y algo o toda la potencia incidente no entra al segundo material. Las ondas que no penetran al segundo medio se reflejan.” [13]

Esto quiere decir que la señal al colisionar con una estructura que se encuentra en su camino retrocede por donde vino si el tamaño de la onda no es tan grande como la superficie que colisiona.

1.5.9.2 Distorsión

“La distorsión por intermodulación es la generación de cualquier frecuencia o producto cruzado no deseado, cuando se mezclan dos o más frecuencias en un dispositivo no lineal.” [13]

1.5.9.3 Difracción

“Ocurre en el borde de un cuerpo impenetrable que es grande en comparación con la longitud de onda de Radio. Cuando la longitud de onda se encuentra con un borde de este tipo, las ondas se propagan en diferentes direcciones con el borde de la fuente.” [11]

Otras propiedades ópticas de las ondas de Radio tenemos: interferencia, refracción, ensombrecimiento, absorción atmosférica.

1.5.10 Estandarización

Para garantizar el intercambio de información eficiente a través del canal de comunicaciones, la selección, creación de mejores equipos para la transmisión de acuerdo con normas específicas a nivel global que se establecen entre otros aspectos, se crearon los estándares. [14]

1.5.10.1 Organizaciones de estandarización

“Los estándares son documentos que proporcionan especificaciones principalmente sobre la tecnología,” [14] que ayudan a impulsar la innovación, y el desarrollo detallado de los circuitos integrados, equipos o productos.

“Hay una serie de organizaciones involucradas en la creación de especificaciones y estándares técnicos, así como en la regulación en el área de las comunicaciones móviles. Estos pueden dividirse en tres grupos: Organizaciones de desarrollo de estándares, organismos reguladores y administraciones, y foros de la industria.” [15]

1.5.10.1.1 Las organizaciones de desarrollo de estándares (SDO)

“Desarrollan y acuerdan estándares técnicos para sistemas de comunicaciones móviles, con el fin de hacer posible que la industria produzca e implemente productos estandarizados y proporcione interoperabilidad entre esos productos.” [15] Un ejemplo:

1.5.10.1.1.1 3GPP (Third Generation Partnership Project)

Según CISA (2021), “Los 3rd Generation Partnership Project (3GPP), es una organización de estándares de telecomunicaciones, desarrolla una serie de lanzamientos que brindan a los desarrolladores una plataforma para la implementación de funciones de telecomunicaciones celulares.”

Según Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) “la tecnología 3GPP de estos grupos se desarrollan continuamente en sucesivas generaciones “G” de sistemas móviles y celulares comerciales, 3GPP ha sido el punto focal para la mayoría de los sistemas móviles.” [30] Desarrollando principios y arquitecturas de Seguridad 2G/3G/4G y algoritmos. [18]

Según Dahlman E., Parkvall S., Skôld J. (2018), “es una organización global de siete SDO[27] regionales y nacionales en Europa (ETSI-Instituto Europeo de Normas de Telecomunicaciones), Japón (ARIB y TTC), Estados Unidos (ATIS), China (CCSA), Corea (TTA) e India (TSDSI).” [15] “3GPP se creó en 1998.” [17] “Proporciona a sus miembros un entorno estable para producir informes y especificaciones que definen las tecnologías 3GPP,” [14] “actualmente 3GPP es la única organización importante que desarrolla especificaciones técnicas para comunicaciones móviles.” [15]

[27] Organizaciones industriales sin fines de lucro… que redactan estándares dentro de un área determinada bajo el mandato del gobierno.” [15]

“Los objetivos de la colaboración fueron desarrollar una visión para una red inalámbrica totalmente IP que cubra el acceso por Radio / redes centrales, capacidades de servicio e interfuncionamiento con redes Wi-Fi”[17] “, incluidas TDD, Dúplex por División de Frecuencia (FDD)” [17] que es la operación de espectros emparejados y no emparejados dentro de un Radio común. [28]

1.5.10.1.1.1.1 Proceso de estandarización

“Las especificaciones 3GPP están estructuradas como versiones y el trabajo de estandarización se basa en contribuciones. Las especificaciones se publican hasta cuatro veces al año después de las reuniones plenarias trimestrales. Las empresas participan a través de su membresía en un socio organizativo 3GPP. Cada versión consta de varios informes técnicos y especificaciones, cada uno de los cuáles puede haber pasado por muchas revisiones. A menudo, una versión proporciona una nueva tecnología de acceso de Radio y/o avances a una existente.” [14] Cuando una versión es publicada no se pueden realizar cambios técnicos, hasta la siguiente versión, porque se “congela.” [16][30]

1.5.10.1.1.1.2 Evoluciones de las versiones 3GPP

(Véase la Figura 15), en la página 29 “Migración de 3GPP Rel 99 a Rel 16.

1.5.10.1.1.1.2.1 Versión 99

Fue la primera versión de 3GPP basado en 3G. [17][19] “La versión 99 se completó en el 2001 y se especializo en la primera tecnología de Radio 3G basado en el Sistema Universal de Telecomunicaciones Móviles UTMS que incorpora una Interfaz Aérea CDMA.[28]” [14]

1.5.10.1.1.1.2.2 Versión 99, 4 - 7

Son exclusivos al especificar 3G. [17]

1.5.10.1.1.1.2.3 Versión 8

[28] “Code División Múltiple Access propuesta por Qualcomm en 1989.” [20]

“Se publicó en diciembre del 2008. 3GPP introdujo la tecnología LTE por primera vez. Evolved Packet Core (EPC) es definida por 3GPP en la Versión 8, por lo que el modo de datos de conmutación de circuitos se vuelve inoperante. Adopta 4 × 4 Sistema MIMO, Acceso múltiple por División de Frecuencia Ortogonal (OFDMA) en DL y Acceso Múltiple por División de Frecuencia de Portadora Única (SC-FDMA) en UL.” [17]

1.5.10.1.1.1.2.4 Versión 9

Trajo mejoras a LTE, se publicó en diciembre del 2009. “Se especificaron tres esquemas de posicionamiento: Sistema de Posicionamiento Global Asistido (A-GPS); Diferencia Horaria de Llegada Observada (OTDOA): e ID de Celda Mejorada (E-CID).” [17] Usados para determinar con precisión la ubicación de un usuario durante un desastre natural y casos de emergencia. [17]

Se agregaron mejoras al concepto de red autoorganizada (SON), con un enfoque en la autoconfiguración del Nodo B (eNB) Evolucionado. Los servicios de Multidifusión de Difusión Multimedia Evolucionados (eMBMS) se describieron en la Capa Física en la versión 8, pero la versión 9 completó las especificaciones para la Capa de Red y los aspectos de la Capa Superior. Se extendió la Formación de Haces a Múltiples Capas (Usuarios Múltiples) y se introdujo el Sistema de Alerta Móvil Comercial (CMAS) además del Sistema de Alerta de la Tierra y los Tsunamis (ETWS) introducido en la versión 8.” [17]

1.5.10.1.1.1.2.5 Versión 10

“Fue publicado en marzo del 2011 describió LTE-Advanced. Esta versión de 3GPP implementa una combinación de Células grandes (Macro) y Células pequeñas, comúnmente conocidas como Redes Heterogéneas (HetNet). Además, aumentó el número de antenas en el sistema MIMO hasta 8× 8 MIMO en DL y 4 × 4 en UL (lado del usuario). Proporcionó itinerancia mundial con una alta eficiencia espectral, la Agregación de Portadoras (CA), que los operadores pueden usar para emplear su espectro fragmentado disperso en bandas diferentes o iguales para mejorar el rendimiento del usuario al transportar datos simultáneamente sobre dos o más portadoras. Otra mejora fue la coordinación mejorada de interferencia entre Celdas (eICIC) para gestionar los problemas de interferencia en HetNet[29].

[29] *Véase Figura 8.*

1.5.10.1.1.1.2.6 Versión 11

“Publicada en Septiembre de 2012, la versión 11 agregó más mejoras a LTE-Advanced, como la Introducción del Multipunto Coordinado (CoMP), que permite a los transmisores compartir la transmisión y recepción de carga de datos incluso si los alojados de forma remota están conectados por enlace de fibra. Se propuso un Canal de Control de Enlace Descendente físico mejorado (ePDCCH) para aumentar la capacidad del canal de control. La versión define un método en el que el dispositivo de usuario (UE) informa a la red si necesita operar en modo de ahorro de batería o en modo normal. " [17]

1.5.10.1.1.1.2.7 Versión 12

“Publicada en Junio de 2014, la versión 12 recomendó más mejoras en LTE-Advanced, la optimización y mejoras de las Celdas pequeñas, incluida su implementación en áreas densas.

Además, la versión 12 introdujo CA entre sitios entre Macrocélulas y pequeñas, también conocida como conectividad dual. También se centró en la comunicación de tipo de máquina (MTC) que creó enormes problemas de capacidad y señalización de red, por lo que se definió una nueva categoría de UE para las operaciones de MTC optimizadas. Así como operar en espectro sin licencia, ya que brinda muchos beneficios a los operadores, como una mayor capacidad de red y un mejor rendimiento.” [17]

1.5.10.1.1.1.2.8 Versión 13

“La versión 13, también conocida como versión inicial de LTE-Advanced Pro, se publicó en Diciembre de 2015. La versión 13 introdujo tres categorías de tecnología importantes: entre ellas FD-MIMO. La idea clave de FD-MIMO era emplear una gran cantidad de antenas dispuestas en un panel de matriz de antenas 2D y recursos de frecuencia adicionales mediante la adopción de CA de hasta 32 portadoras de componentes (CC) en comparación con solo hasta 5 CC en la Versión 10. Además, admitía hasta 8 antenas MIMO según las versiones anteriores, pero prometía examinar sistemas MIMO de alto nivel con hasta 64 antenas MIMO.

La versión 13 propuso posibles mejoras para la transmisión multiusuario DL utilizando codificación de superposición. El Internet de las cosas de Banda Estrecha (NB-IoT) se estandarizó para proporcionar conectividad de área amplia para comunicaciones masivas de tipo máquina (mMTC).” [17]

1.5.10.1.1.1.2.9 Versión 14

“Publicado en Junio del 2017, conocido por el inicio inicial de la estandarización 5G. Algunas áreas principales incluyen la reducción de latencia a 1 ms para mejorar la experiencia del usuario final en comparación de los 5 ms en la versión 8 para paquetes IP en condiciones ideales de Radio. Proporciona soporte completo para las transmisiones UL en espectro sin licencia para construir el marco de conectividad dual recomendado en la versión 13.

Analizó nuevos casos de uso como los Sistemas de Transporte Inteligente (ITS).” [17]

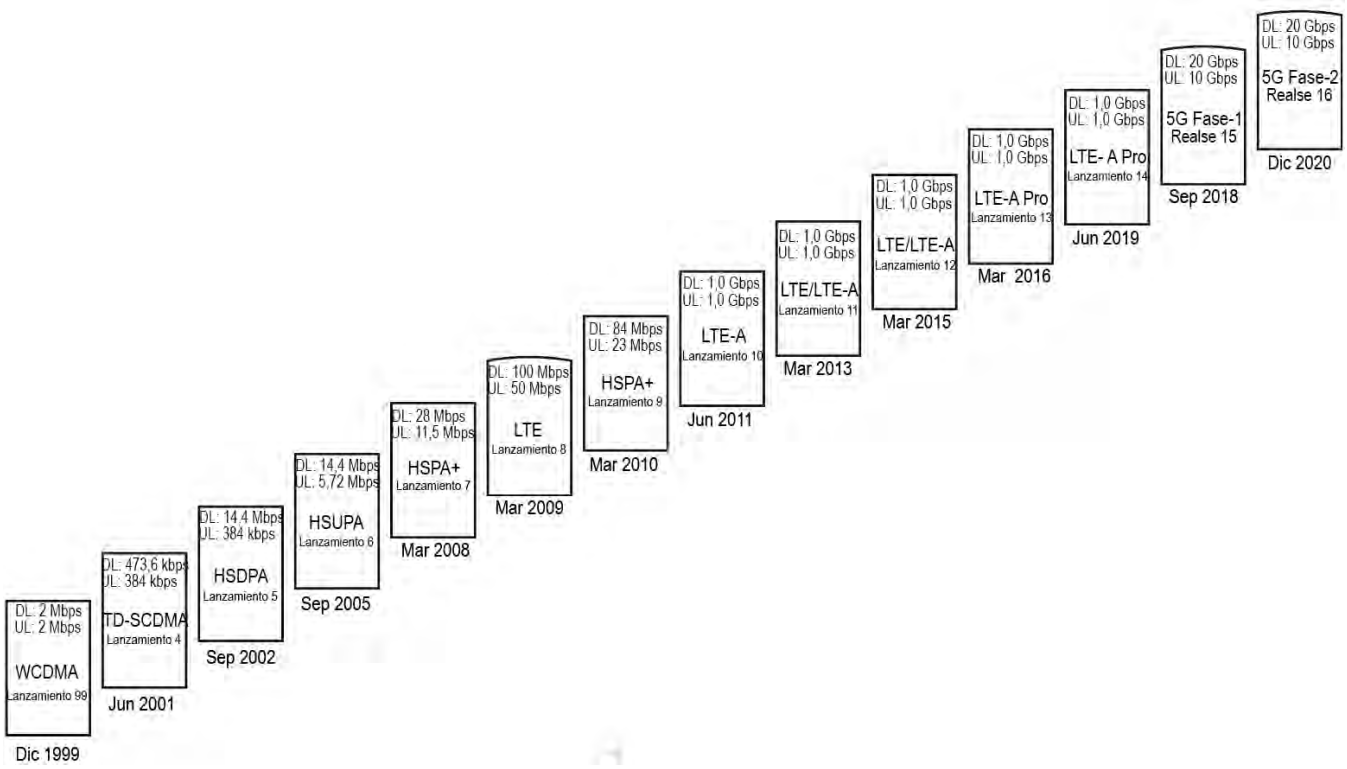


Figura 15 Migración de 3GPP Rel 99 a Rel 16. Fuente: Saad Z. Asif (2019) [14]

(Véase la Figura 15) la evolución de los lanzamientos de las versiones de 3GPP desde 1999 al 2020.

1.5.10.1.1.2 3GPP2

Es una organización de estandarización que ofrecía servicios a la 3G, pero de manera alternativa, este proyecto dio origen a la evolución de IS-95 a CDMA en el año 2000 llamado CDMA-2000, no tiene relación con 3GPP porque trabajaron de manera paralela, aun así, 3GPP dominó el área por completo en 4G y 5G en los próximos años. [15]

1.5.10.1.2 Organismos reguladores y administradores

"Son organizaciones dirigidas por el gobierno que establecen requisitos reglamentarios y legales para vender, implementar y operar sistemas móviles y otros productos de telecomunicaciones." [15]

Estas organizaciones se dedican a:

- Certificar los equipos de telecomunicaciones móviles verificando si cumplen con requisitos específicos para operar.
- Controlar el uso de licencias de los operadores móviles para usar partes de la red.
- Controlar el espectro, dependiendo de los servicios que se utilizarán se asigna a través de organismos regionales como: Europa (CEPT / ECC), América (CITEL) y Asia (APT). "A nivel mundial, dicha regulación está a cargo de Unión Internacional de Telecomunicaciones (UIT)." [15]

1.5.10.1.2.1 UIT

"La Unión Internacional de Telecomunicaciones (UIT) es un organismo de normalización," [18] "con una variedad de requisitos y estándares globales relacionados con las telecomunicaciones," [18] estos estándares los registra en las IMT dependiendo la Generación Móvil.

1.5.10.1.2.2 UIT-R

“El sector de Radiocomunicaciones de la UIT (UIT-R) se centra en aspectos de Sistemas Inalámbricos y de Radio.” [20]

“Desarrolla reglamentos y normas de radiocomunicaciones para asegurar el rendimiento y calidad necesarios en el funcionamiento de los sistemas de radiocomunicaciones. Es responsable para la gestión global del espectro de frecuencias de Radio y los recursos de la órbita de los satélites.

El objetivo principal es garantizar el uso económico, eficiente y sin interferencias en los sistemas de radiocomunicaciones. Esto se garantiza mediante la implementación del Reglamento de Radiocomunicaciones.” [14]

Esto quiere decir, que el Sector de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones, a través de las conferencias Mundiales de Radiocomunicaciones (CMR) asigna las frecuencias para las comunicaciones móviles. [14]

1.5.10.1.3 Foros de la industria

Es un grupo de operadores y proveedores que crean foros en la Industria, promoviendo la tecnología de comunicaciones móviles, por ejemplo: [14]

1.5.10.1.3.1 GSMA

GSMA (Asociación GSM) basado en GSM, WCDMA, LTE y NR. [14]

1.5.10.1.3.2 WCDMA

“Es el sucesor de GSM, CDMA de banda ancha. [20] Puede admitir Alamouti[30] 2x2 esquema MIMO,[31] [17] “es el único código de espacio-tiempo ortogonal.” [17]

1.5.10.1.3.3 5G Américas

[30] “Es el único código de espacio-tiempo ortogonal con tasa 1.” [17]
[31] “Se refiere al uso de múltiples antenas tanto en el transmisor como en el receptor.” [20]

“Es un foro regional de la industria que ha evolucionado a partir de su predecesor 4G Américas.“ [15]

1.5.11 Evolución de la Telefonía

“Las tecnologías de comunicaciones móviles en evolución nos brindan velocidades de datos cada vez mayores, tiempo de respuesta más rápido y medios cada vez más fluidos para acceder a más contenido que nunca en la historia de las telecomunicaciones,” [18] por eso están en constante cambio (Kaizen) para ofrecer equipos de alta calidad con características innovadoras, de acuerdo con las necesidades y expectativas de los clientes, impulsando la compra de los equipos. En esta sección nos encontramos con las generaciones móviles desde la generación cero a la cuarta generación con sus características que los diferencian entre sí.

1.5.11.1 0G

Es la generación “Con una base de usuarios relativamente pequeña y una portabilidad limitada.” [18]

Tabla 5 Generación 0 ejemplo 1. Fuente: Elaboración propia basado en Jyrki T. J. Penttinen (2019)[18]

Fecha	“1956 MTA Automático Sueco Sistema de telefonía móvil versión A.” [18]
Descripción	“Equipo voluminoso, era adecuado simplemente para un entorno montado a un automóvil.” [18]
Ubicación	Estocolmo y Gotemburgo. [18]

Tabla 6 Generación 0, ejemplo 2. Fuente: Elaboración propia basado en Jyrki T. J. Penttinen (2019) [18]

Fecha	“1971 ARP (Auto Radio Phone).” [18]
Descripción	“Funcionó en la banda 160 MHz hasta 2000, sirviendo especialmente a clientes en áreas remotas.” [18]
Ubicación	Finlandia. [18]

1.5.11.2 1G Primera Generación Móvil

Tabla 7 Primera Generación Móvil, estructura básica. Fuente: Elaboración propia basado en [15][17][18][19][20][21][22]

Fecha	1980. [18]
Descripción	Primera generación de comunicación móvil. [15]
Primeros desarrolladores	Estados Unidos, Japón y algunas ciudades de Europa. [20]
Características	• "Equipos de usuario montado en vehículo que también podía usarse como dispositivos portátiles." [18] • Comunicación analógica. [19][20] • Pesaba varios kilogramos, tenía un auricular por separado. [18] • No estaba diseñado para bolsillos. [18] • Su capacidad era muy limitada. [18]
Impulso	• Para liberar a los usuarios de ubicaciones fijas. [18] • Simplemente ofrecer servicios de voz analógico sin Seguridad. [17]
Inconvenientes	Las llamadas se suspendían en determinados periodos de tiempo, provocando la frustración por parte de los usuarios ya que interrumpía la comunicación en tiempo real, sumándole la duración de la batería del equipo. [17]
Nuevas funcionalidades	Voz. [22]
Algunos estándares	• AMPS (Sistema de Telefonía Móvil Avanzado) en Norteamérica [18][15] Implementado también en Europa y Japón por ETACS. • TACS (Sistema de Comunicaciones de Acceso Total) en Reino Unido. [18] [15] • NMT 450 (Telefonía Móvil Nórdica) [15] y su versión mejorada [10] era controlado por el gobierno. [15] • NMT 900 Versión más actualizada de NMT. [18]

	• Otro Netz-C. [18] *(Véase Figura 18) "Algunos ejemplos de Sistemas de Comunicaciones Móviles por Generación" que se encuentra dentro del tema "Estandarización de Generaciones Móviles", en las páginas 49 - 51.*
Velocidad de datos	*(Examine la Figura 20) [18] "Desarrollo de las tarifas de Datos Móviles" dentro del tema: "Velocidades de los estándares de generaciones móviles," en las páginas 51 - 52.*
Velocidad de descarga	2 kb/s. [21]
Latencia	N/A. [21]
Seguridad	No contaba con Seguridad. [20] *Véase tema: "Evolución de Amenazas y Seguridad en Generaciones Móviles" en las páginas 59 – 62, Tabla 19 y (la Figura 25.)*
3GPP	N/A. [17] V*éase "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.*

1.5.11.3 2G Segunda Generación Móvil

Tabla 8 Segunda Generación Móvil, estructura básica. Fuente: Elaboración propia basado en: [14][15][17][18][19][20][21][22].

Fecha	1990. [18][19]
Descripción	Segunda generación de comunicaciones móviles. [15]
Tipo de señalización	• Codificación de desplazamiento mínimo gaussiano (MSK). [17]
Características	• Introducción digital en el enlace de Radio [15] utilizando códecs de voz digitales. [20] • Servicios de datos limitados. [15]

	• Otra parte involucrada con GSM es Enhanced Data Rates for GSM Evolution (EDGE) que utilizó modulación 8PSK. “Edge ofrece una velocidad de datos de Radio por intervalo de tiempo igual a 69,2 kb/s una velocidad máxima de datos de usuario.” [17] • Uso del enfoque de Acceso Múltiple por División de Tiempo Digital (TDMA), [19] capaz de multiplexar a varios usuarios en la misma frecuencia por turnos específicos. [17][20] • Multiplexación[32] por División de Código (CDM) [18] para multiplexar varios usuarios utilizando un solo canal. • Ambas Bandas de Frecuencia DL (Enlace Descendente) y UL (Enlace Ascendente) están en las bandas 900 MHz y 1.8 GHz en Europa. [17]
Tipo de conmutación de datos	• “Conmutación por circuitos para servicios de voz y datos de baja velocidad en bits,” [19] “que adopta canales de radiofrecuencia.” [17] • Transmisión de datos por conmutación de paquetes, punto de partida para las comunicaciones móviles hacia el entorno IP. [18]
Impulso	• “Aumentar la capacidad del sistema añadiendo servicios adicionales como SMS e identificador de llamadas, mejorar la Seguridad, reducir el costo.” [17] • Eficiencia de espectro. [20] • Añadir Roaming Internacional. [20]
Nuevas funcionalidades	• Integración de servicios de Voz, y mensajería (SMS) [18] [22] MMS (Mensajes Multimedia) [20]. El primer SMS se envió el 3 de diciembre de 1992 en Reino Unido. [20] • Roaming Internacional. [20] • Conferencias. [20]

[32] Varios usuarios transmitiendo en la misma frecuencia.

	• Llamada en espera, retención de llamadas, desvío de llamadas, restricción de llamadas, identificación del número de la persona que se llama, grupos de usuario. [17]
Estándares	• GSM (Sistema Global para Comunicaciones Móviles) [19] Estandarizada en Europa por 3GPP. Incluye GSM900, GSM-R, GSM1900, GSM400. [20] GSM "Introdujo la separación de la terminal y el almacenamiento de datos del abonado (SIM) (Modulo de Identidad del abonado) para facilitar el cambio de dispositivo conservando el mismo número." [10] Se extendió desde Europa a otras partes del mundo. [15] Estándares GSM • IS-54 (Interim Standard). [19] • IS-136. [19] • IS-95 basado en CDMA en América del Norte [10] alternativa de IS-54, [20] "varios usuarios comparten la misma Banda de Frecuencia al mismo tiempo." [20] El sucesor de IS-95 es CDMA2000. [20] • D-AMPS (Digital AMPS). [15] • PDC (Comunicación personal digital). [15][19] GPRS (Servicio General de Radio por paquetes) es una versión mejorada de GMS, integrando una red IP basada en Datagram Packet Switching para proveer servicios en base a IP e interconexión de Internet, [19] creado por ETSI en 1990. [20] *(Examine Figura 18) "Algunos ejemplos de Sistemas de Comunicaciones Móviles por Generación" que se encuentra dentro del tema "Estandarización de Generaciones Móviles", en la página 50.*
Velocidad de datos	*(Véase Figura 20) [18] "Desarrollo de las tarifas de Datos Móviles" dentro del tema: "Velocidades de los estándares de Generaciones Móviles," en las páginas 51 - 52.*

Tasa de Transferencia de datos máxima	38,4 kb/s en una Red GSM 900. [17]
Latencia	629 ms. [21]
Frecuencia	Bandas de Frecuencia UL y DL están en las bandas 900 y 1.8 GHz en Europa. [17]
Organización Celular	"Por Femtocélula, admite estándares de Radio GSM, GRPS y EDGE." [14] *Véase tema: Organización Celular" en la página 16 - 18.*
Banda de frecuencia	De 800MHz a 1900 MHz [14] con una sola antena.
Seguridad GSM cifrado aéreo	IMSI, Ki, Algoritmos: A3, A8, A5. [20] *Examine tema: "Evolución de Amenazas y Seguridad en Generaciones Móviles" en las páginas 62 - 64, Tabla 20, 21, (ver Figura 26.)*

1.5.11.4 3G Tercera Generación Móvil

Tabla 9 Tercera Generación Móvil, estructura básica. Fuente: Elaboración propia basado en [14][15][17][18][20][21][22].

Fecha	• 2000 [15]
Descripción	Tercera generación de comunicación móvil. [15]
Características	• Sistemas con capacidad multimedia. [18] • Rápido acceso inalámbrico a Internet. [15] • Posibilidad de utilizar velocidades de datos considerablemente más altas. [18] • Etapa inicial del LTE. [18]

	• LTE (Long-Term Evolution) “Es el representante más popular y estuvo disponible por primera vez alrededor de 2010-2011, ofrece una mejor eficiencia espectral que cualquier sistema anterior.” [18] • WiMax es otro representante en la ruta 3G avanzada. [18] • Implementación de CDMA2000 estadounidense.[18] Evolución de IS-95. • “Los dispositivos móviles fueron reemplazados por teléfonos inteligentes.” [20]
Impulso	• “Necesidad de velocidades de datos más altos como base para el consumo fluido de servicios multimedia cada vez más avanzados.” [18] • Mejor eficiencia espectral de los sistemas post - 2G. [18] • Mejorar el rendimiento del procesador. [18]
Nuevas funcionalidades	Voz, Email, multimedia. [22]
Tipo de conmutación de datos	Conmutación de paquetes RAN (Radio Access Network) basada en IP e IP Core. [20]
Estandarización	IMT-2000 (Telecomunicaciones Móviles Internacionales). “Conjunto de sistemas 3G comerciales según la UIT.” [18] También está alineada a 1G y 2G. [18] • DECT (Digital Enhanced Cordless Telecomunications) Telecomunicaciones inalámbricas Mejoradas Digitales. [18] • HSPA (High Speed Packet Access) [15] de UTMS [18] en 2010 [17] permite el rápido acceso a Internet. • CDMA2000 junto con EDGE (Enhanced Data rates for Global Evolution) Velocidades de datos mejoradas para la evolución global.[18] El antecesor de CDMA2000 es IS-95. [20]

	(Examine Figura 18) "Algunos ejemplos de Sistemas de Comunicaciones Móviles por Generación" que se encuentra dentro del tema "Estandarización de Generaciones Móviles", en la página 50.
Velocidad de datos	*(Véase Figura 20) [18] "Desarrollo de las tarifas de Datos Móviles" dentro del tema: "Velocidades de los estándares de Generaciones Móviles," en las páginas 51 - 52.* • UMTS/WCDMA con la Interfaz de Radio ofrecía para DL de 384 kb/s a 2Mb/s. [17] • El acceso a paquetes de alta velocidad (HSPA) mejoró de 14,1 Mb /s DL y 5,76 Mb en UL. [17] • La actualización de HSPA, es decir HSPA+, de 168 Mb/s en DL y 22 Mb/s en UL. [17]
Velocidad de descarga	56 Mb/s. [21]
Latencia	212 ms. [21]
Organización Celular	• "Femtocélula, por tecnología dual 2G/3G." [14] • "Por UMTS, para ampliar la cobertura WCDMA y la capacidad HSPA en residencias. Permiten servicios como aplicaciones basadas en ubicación. [14] • Por CDMA2000, admiten estándares CDMA2000 1x y CDMA 1Xev-do." [14] • "La Celda pequeña está conectada a una Red Central GSM mediante IPSec, (Seguridad IP) garantizando la Seguridad entre la Celda pequeña y el operador." [14] *Examine tema: "Organización Celular", en la página 16 – 18.*
Seguridad	Implementación de estándares según la UIT en IMT-2000, Políticas de Seguridad, así como medidas de Seguridad en Sistema Operativo de dispositivo móvil. [20]

	Examine tema: "Evolución de Amenazas y Seguridad en Generaciones Móviles" en las páginas 64 - 66, Tabla 22.
3GPP	3GPP incorporó el Servicio de difusión y Multidifusión Multimedia (MBMS) en combinación con el Sistema Multimedia de Protocolo de Internet (IMS). [17] Versión 99, 4 a Versión 7. [17] *Véase "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.*

1.5.11.5 LTE

La transición entre 3G y 4G se llamó LTE. "LTE es la tecnología de Red de Acceso por Radio estandarizada que utiliza IP como protocolo de transporte para todos los servicios, incluyendo la telefonía." [19] Las implementaciones del LTE comenzaron en el 2010, [17] pero comenzó a desarrollarse a partir del 2004, con el propósito de implementar una nueva tecnología de Acceso por Radio Centrada llamada C-RAN, únicamente en datos conmutados por paquetes. [15]

1.5.11.5.1 Tecnologías LTE

Para poder satisfacer la demanda de servicios con mayor rendimiento, que millones de usuarios utilizaban cada día, LTE integró algunas tecnologías importantes de Radio y redes centrales, entre ellas podemos encontrar: [20]

Tabla 10 LTE. Fuente: Elaboración propia basado en Madhusanka Livanage (2018) [20]

Tipo de Multiplexación	Descripción
OFDM Multiplexación por División	• "Proporciona altas velocidades de datos." [20] • "Redujo la complejidad computacional debido a la implementación de la Transformada de Rápida de Fourier (FFT)." [20] • Soporte de servicios de radiodifusión. [20]

de Frecuencia Ortogonal [12]	• Esquema de múltiples portadoras eficientes. [20]
FDMA (Acceso Múltiple por División de Frecuencia) [12]	• "Ofrece Ancho de Banda para dar servicio a varios usuarios" [20] asignando un rango de frecuencia a cada usuario. La utilización del método de transmisión (SC-FDE) para la ecualización de frecuencia de portadora única, utilizado para transmitir datos a través de la Modulación de Amplitud de Cuadratura (QAM), [20] que es una técnica de modulación digital.
Técnica de Múltiples Antenas [12]	• "Proporciona soluciones de capacidad del sistema, solidez del enlace y eficiencia espectral." [20] Sirve para combatir el desvanecimiento de la señal por trayectos múltiples amplificando el patrón de radiación de la antena. La Formación de Haces para que las señales transmitidas hacia la dirección más eficiente del receptor, reduciendo la relación señal - ruido. [20]

Tabla 11 LTE 3GPP y Seguridad. Fuente: Elaboración propia, basado en [17][20]

3GPP	"3GPP se publicó en diciembre del 2008 e introdujo la tecnología LTE por primera vez." [17] V*éase "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.*
Seguridad en LTE	Cifrado de la señal de tráfico y mensajes. [20] *Examine tema: "Evolución de Amenazas y Seguridad en Generaciones Móviles" en la página 66, Tabla 23.*

1.5.11.5.2 Evolución LTE

LTE Actualmente continúa evolucionando, ya que es un componente importante en el Acceso de Radio 5G, en la Tabla 12 podemos ver la evolución de LTE de acuerdo con los lanzamientos hechos por 3GPP, introduciendo funciones y capacidades adicionales en cada lanzamiento. [15]

Tabla 12 Versiones LTE mediante lanzamientos de 3GPP. Elaboración propia basado en [15]

Lanzamiento 3GPP	Descripción	Año			Objetivo de evolución
		Completó	Operación	Finalización	
Versión 8	Es la primera versión de LTE. [15] Es la base de versiones posteriores LTE. [15]	2008. [15]	2009. [15]		
Versión 9	Es la base de versiones posteriores LTE. [15]				
Versión 10	Es la primera versión de LTE-Advanced, [15] el comienzo de la evolución. [15]	2010. [15]			Garantizó que la tecnología de Acceso de Radio LTE cumpliera con los requisitos de IMT-Advanced. [15]

Versión 11				2012. [15]	
Versión 12		2014. [15]			
Versión 13	Es la primera versión de LTE-Advanced Pro, [15] O llamada 4.5G. [15]			2015. [15]	Paso tecnológico intermediario entre 4G y la Interfaz Aérea 5G NR. [15]
Versión 14		2017. [15]			
Versión 15		2018. [15]			

Tabla 13 Área de evolución LTE de acuerdo con los lanzamientos 3GPP. Fuente: Elaboración propia basado en: [15].

Lanzamiento 3GPP	Áreas de evolución
Versión 8	
Versión 9	
Versión 10	Mayor flexibilidad del espectro: • A través de agregación de portadoras. • Transmisión de múltiples antenas. • Mejoras en la coordinación de interferencias entre celdas en redes Helnet. [15]
Versión 11	• Funcionalidad de Radio Interfaz para multipunto coordinado (CoMP) transmisión y recepción. • Agregación de portadoras. • Nueva estructura de canal de control (EPDCCH). [15]
Versión 12	Se centró en celdas pequeñas con características como:

	• Conectividad dual. • Encendido/apagado de celdas pequeñas. [15]
Versión 13	• Nuevos escenarios de comunicación de dispositivo a dispositivo V2V, V2X M2M, drones teledirigidos. • Acceso asistido por licencia para admitir espectros sin licencia. • Transmisión de múltiples antenas masivas. [15]
Versión 14	Mejoras en la operación de espectros sin licencia. Soporte para: • V2V • V2X Transmisión del área amplia con subportadora reducido. [15]
Versión 15	• Latencia significativamente reducida. • Comunicación mediante Antenas. [15]

En la Tabla 13 podemos ver las áreas de evolución de cada lanzamiento 3GPP basado en LTE.

1.5.11.5.3 Descripción general de LTE desde su Primera Versión

LTE surgió con el objetivo de proporcionar una nueva tecnología de Acceso por Radio centrada basada en datos conmutados por paquetes inclusive la flexibilidad del espectro, en términos de soporte de ancho multibanda y un diseño conjunto FDD/TDD, es decir, el espectro pareado que utiliza Dúplex por División de Frecuencia (FDD) y no pareado utilizando Dúplex por División de Tiempo (TDD). [15]

Además el uso de Macro redes con antenas sobre el tejado y Celdas relativamente grandes. *Véase tema: "Organización Celular" en el inicio del Capítulo, página 16 - 18, para más información de Celdas.* La asignación de UL y DL era asignada a todas las Células por igual. [15]

Tabla 14 Características generales de LTE desde su primera versión. Fuente: Elaboración propia basado en: [15].

Características	Descripción
OFDM	El esquema de transmisión básico en LTE OFDM, permite una complejidad de receptor razonable en combinación con la multiplexación espacial (MIMO) de múltiples antenas y MIMO de usuario único siendo una parte integral de LTE. [15]
Dominio del tiempo	LTE organiza las transmisiones en tramas de 10 ms, cada uno consta de 10 subtramas de 1 ns. La duración de la subtrama de 1ms corresponde a 14 símbolos OFDM, que es la unidad más pequeña de LTE. [15] Para cada subtrama el planificador controla que dispositivos deben transmitir y recibir y en que frecuencia. [15]
Señales de referencia	Las señales de referencia específicas de la celda están constituidas de manera angular dependiendo donde se encuentren cada Estación Base. Las estaciones base al transmitir varias señales de referencia, independientemente si hay datos DL para transmitir o no. [15]
Señales de referencia específicas de la Celda	Las celdas son grandes para que múltiples usuarios puedan acceder a los servicios LTE. Entre las funciones de las señales de referencia basadas en cada celda, tenemos: • La estimación de canal DL para la modulación coherente. • Informes de estado de canal para fines de programación. • Corrección de errores de frecuencia. • Acceso inicial. • Mediciones de movilidad. [15]
Densidad de la señal de referencia	Depende del número de capas que se está utilizando en la trasmisión establecida en cada Célula. [15]
Transmisión de datos	• Se programa de manera dinámica tanto el UL como DL.

	• Se puede seleccionar diferentes velocidades de datos ajustando la velocidad de código del código Turbo, variando la modulación QPSK hasta 64-QAM. [15]

Véase la Tabla 14 las características generales de LTE.

1.5.11.5.4 Modulación de LTE

LTE puede utilizar sistemas de modulación QPSK, 16QAM, 64QAM[18] (ver Figura 16.) El tipo de canal para cada subportadora OFDM individual corresponde al desvanecimiento del plano.

La modulación QPSK proporciona las áreas de cobertura más grandes que la capacidad más baja por Ancho de Banda. 64-QAM da como resultado una cobertura más pequeña, pero ofrece mayor capacidad. [18]

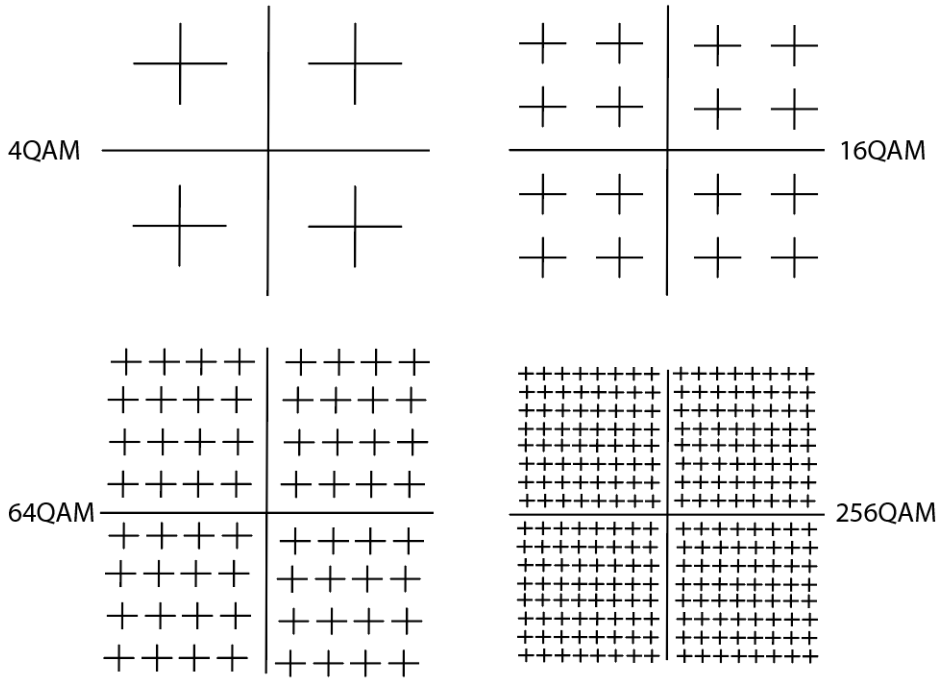


Figura 16 La constelación de QPSK (4QAM) y un conjunto de variantes de QAM relevantes para 5G. Fuente: Jyrki T. J. Penttinen (2019) [18]

1.5.11.5.5 Codificación

LTE utiliza la codificación Turbo o codificación convolucional, la primera es más moderna y proporciona en general una ganancia de aproximadamente 3 dB. [18]

1.5.11.6 4G Cuarta Generación Móvil

Tabla 15 Cuarta Generación Móvil, estructura básica. Fuente: Elaboración propia basado en [15][17][18][19][20][21][22].

Fecha	2008 aprox. [19]
Descripción	Cuarta generación de comunicación móvil. [15]
Beneficios	"Según la UIT; • LTE-Advanced [19] • LTE-Advanced Pro [10][19] • WiMAX-Advance o IEEE 802.16m [19] sólo pertenecen a la categoría 4G." [18]
Nuevas funcionalidades	• Voz. [22] • Email. [22] • Banda Ancha Móvil. [22] • Ya es compatible con M2M e IoT. [19]
3GPP	• 3GPP describe por primera vez LTE-Avanzado en marzo del 2011, [17] desde la versión 10, mejoras en la versión 11 y 12. En la versión 13 la versión inicial de LTE-Avanzado Pro. [17] • Velocidad máxima DL de 100 Mb/s y de • Enlace Ascendente o UL de 50 Mb/s. [17] *Examine tema: "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.*
Estandarización	• IMT-Avanzado. [18] • LTE [15] no es capaz de cumplir con los valores esperados de rendimiento 4G (1Gb/s) en UL [18] LTE admite FDD y TDD. (la operación de los espectros emparejados y no emparejados dentro de un Radio común. [15]

	• HSPA evolucionado [17] HSPA+. • HSPA+ lograr velocidades máximas más altas utilizando MIMO. [20] *(Examine Figura 18) "Algunos ejemplos de Sistemas de Comunicaciones Móviles por Generación" que se encuentra dentro del tema "Estandarización de Generaciones Móviles", en la página 50.*
Velocidad de datos	*(Véase Figura 20) [18] "Desarrollo de las tarifas de Datos Móviles" dentro del tema: "Velocidades de los estándares de generaciones móviles," en las páginas 51 - 52.*
Velocidad de descarga	1 Gb/s [21]
Latencia	60-98 ms. [21]
Macrocélulas	Para incrementar la cobertura proporcionada por la Macrocélula, cada celda se divide en celdas más pequeñas como son el pico celdas. [17]
Tecnologías clave de 4G avanzado	• Mimo mejorado. [20] • Gestión de Ancho de Banda y espectro. [20] • Uso de Ancho de Banda hasta de 100 MHz en bandas de espectro como de de 450 a 470 MHz para ser utilizada en los sistemas IMT. [20] • Asignación de portadoras para utilizar los anchos de banda más amplios de hasta 100 MHz. [20] • Relés[20] "Proporciona cobertura en nuevas áreas, rendimiento en el borde de celda, implementación de Red temporal por ejemplo." [20]
Seguridad 4G	Cifrado de dispositivos móviles, políticas de acceso, recomendaciones para usuarios. [20] Véase *tema: "Evolución de Amenazas y Seguridad en Generaciones Móviles" en la página 67, Tabla 24.*

1.5.12 Línea del tiempo de Generaciones Móviles

(Examine la Figura 16), la organización de lanzamiento de cada generación con fechas aproximadas, juntamente con los estándares más importantes que lo identifican.

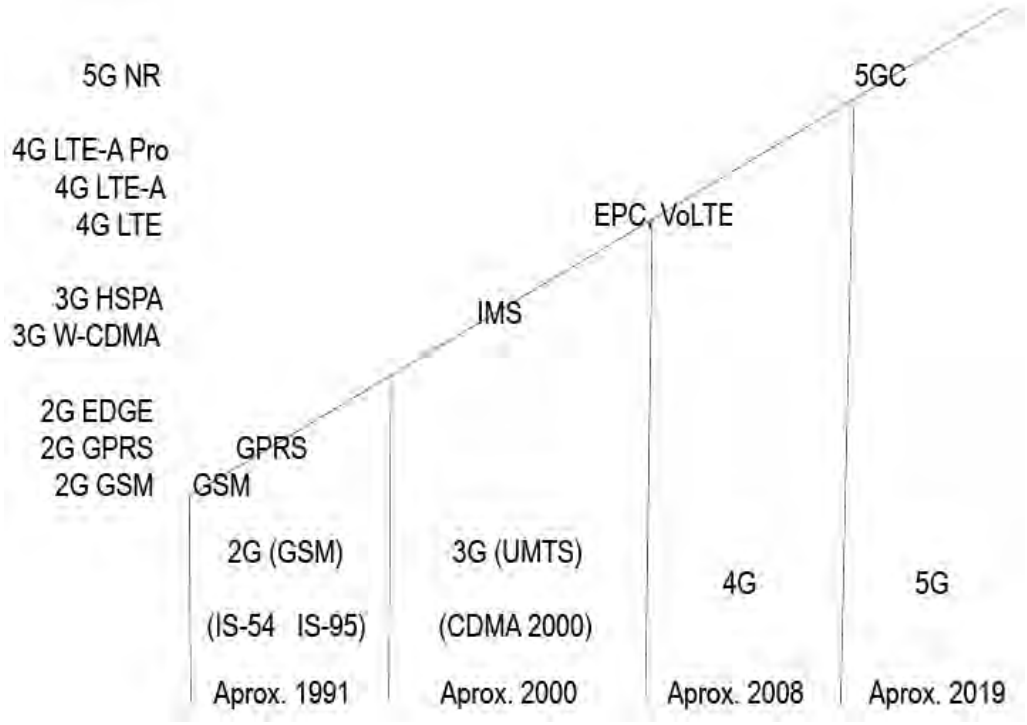


Figura 17 Evolución de Generaciones móviles. Fuente: Ulrick Trick (2021) [19]

1.5.13 Frecuencia

Para las generaciones 2 a 4G utilizan una frecuencia en el rango de “700 MHz hasta por debajo de 3 G GHz.” [20] 3G velocidad de conexión de datos promedio entre 500 y 700 kbps. [12]

1.5.14 Estandarización de Generaciones Móviles

1.5.14.1 IMT

1.5.14.1.1 IMT-2000 (3G)

"Primero referido como *Futuros Sistemas Públicos Terrestres Móviles* (FPLMTS), más tarde pasó a llamarse IMT-2000". [15] Es un conjunto de recomendaciones e informes exclusivos para 3G, se publicó en el 2000 e incluía WCDMA de 3GPP." [15]

Recomendación: UIT-R M.1457 que contiene seis RIT (Tecnología de la Interfaz de Radio) diferentes incluidas las tecnologías de 3G: WCDMA /HSPA. [15]

1.5.14.1.2 IMT-Avanzado (4G)

"IMT-Avanzado es un programa para describir 4G como el próximo paso de la evolución después de IMT-2000," [18] en base a requisitos [20] este incluye nuevas interfaces de Radio que soportan nuevas capacidades de sistemas más allá de las IMT-2000. [18]

La evolución de LTE desarrollada por 3GPP fue una tecnología candidata para 4G. [18]

Recomendación: UIT-R M.2012 que contiene dos RIT diferentes, donde el más importante es 4G/LTE. [15]

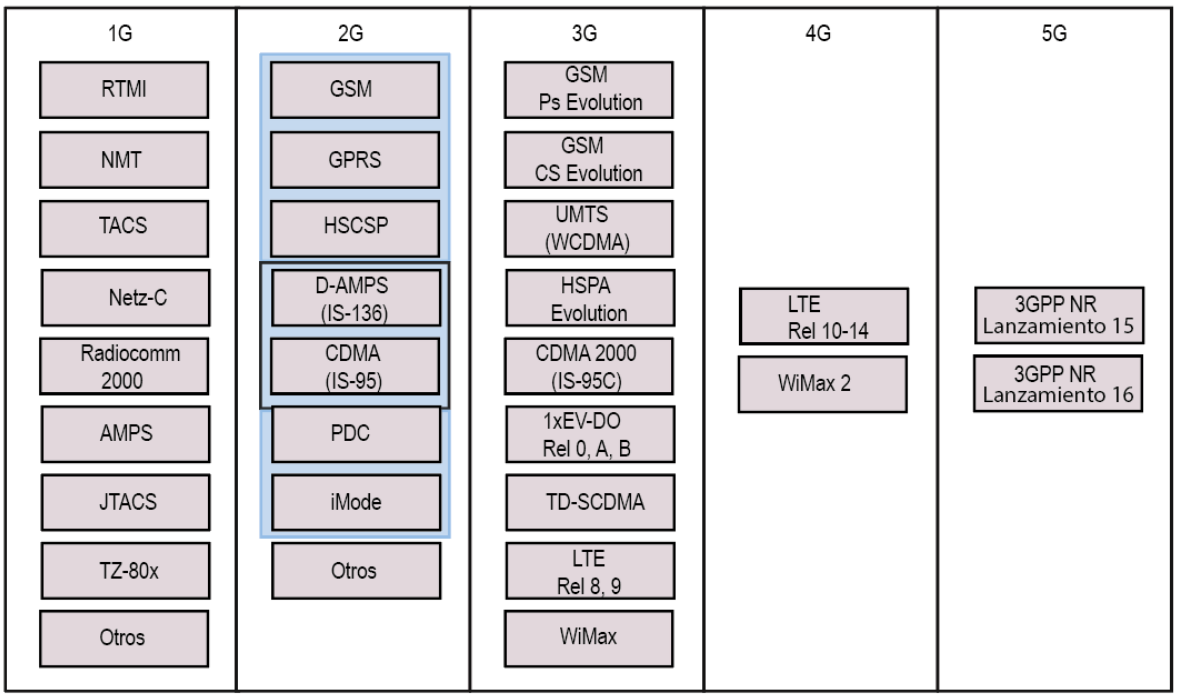


Figura 18 Algunos ejemplos de los sistemas de comunicaciones móviles por generación.
Fuente: Jyrki T. J. Penttinen (2019) [18]

(Examine la Figura 17,) los estándares utilizados para cada generación móvil.

Cada IMT se actualiza periódicamente para reflejar los nuevos desarrollos en las especificaciones detalladas a las que hace referencia, como las especificaciones 3GPP para WCDMA y LTE o en UIT, entre otras. [15]

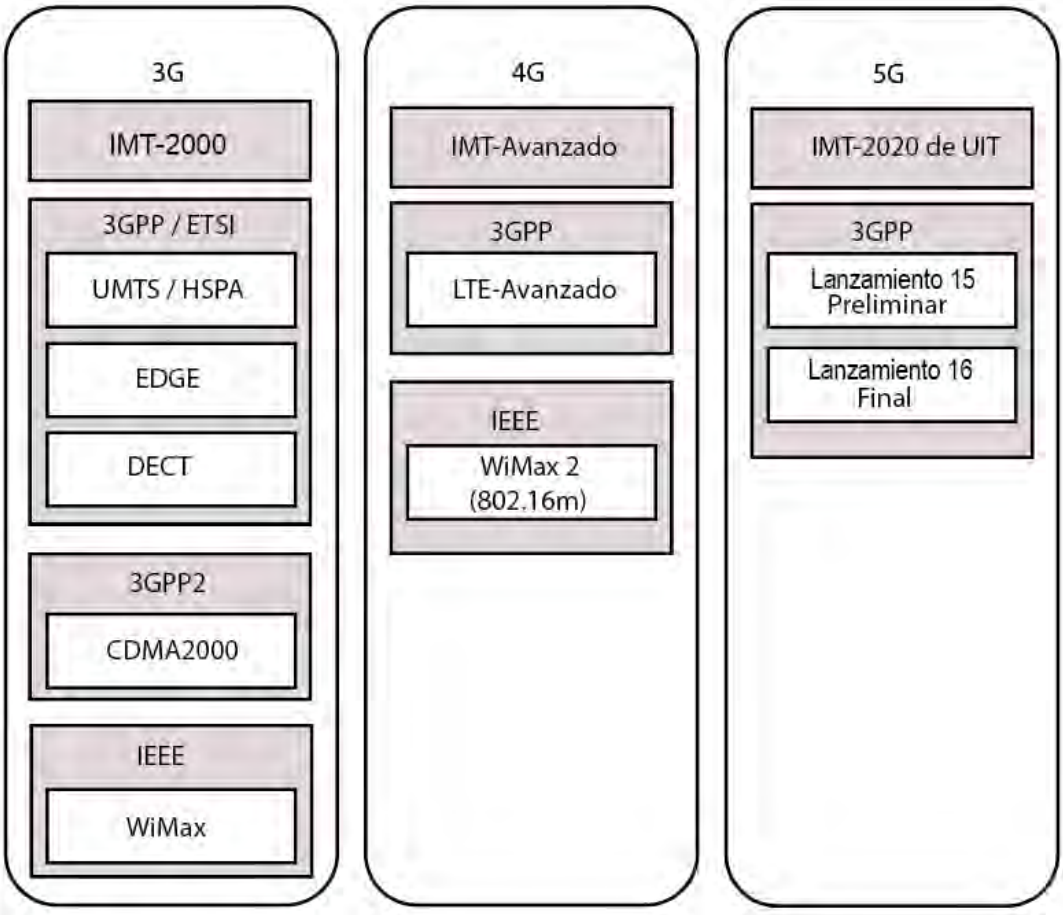


Figura 19 Los principales sistemas de comunicación Móviles 3g y 4g cumplen con los respectivos requisitos de la UIT. Fuente: Jyrki T. J. Penttinen (2019) [18]

Suponiendo un ejemplo de requisitos de los sistemas 4G que se define en IMT-Avanzado, son dispositivos móviles de alta calidad. [20]

(Véase la Figura 19) las IMT de cada generación, con sus perspectivos estándares y las organizaciones que las administran.

1.5.15 Velocidades de estándares de Generaciones Móviles

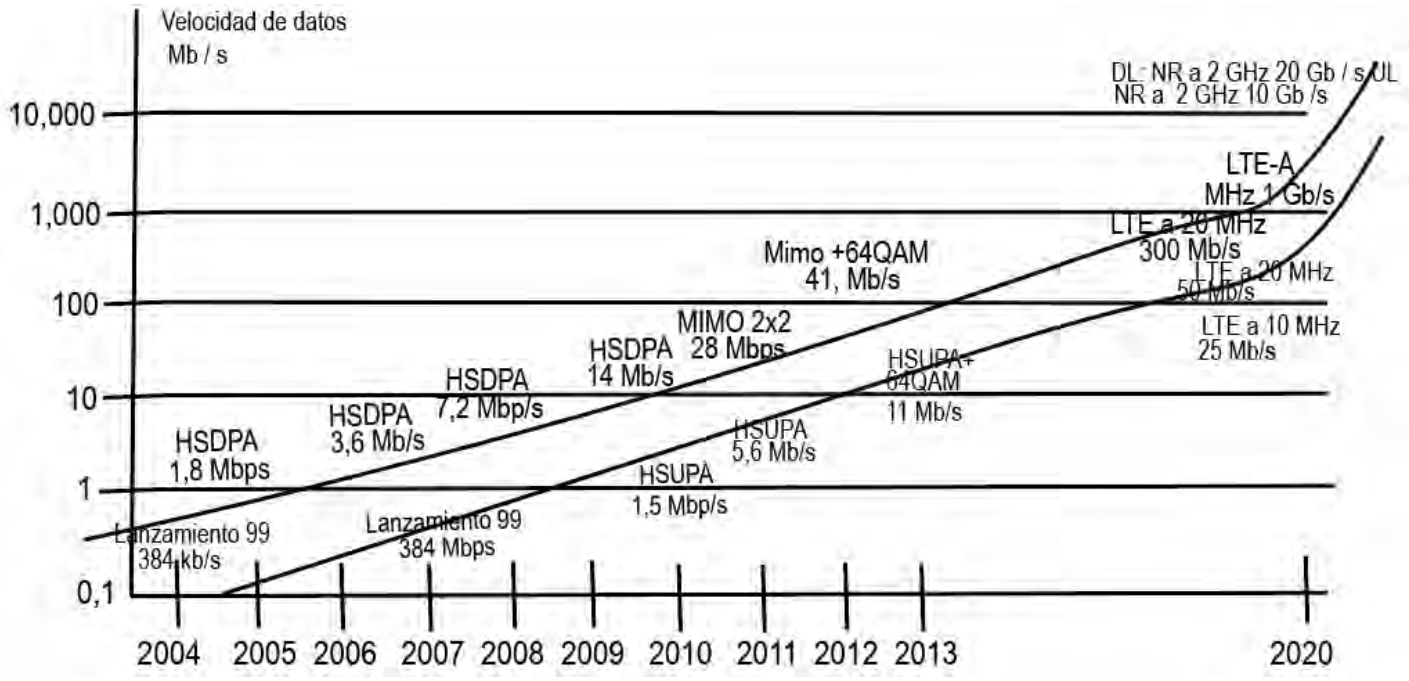


Figura 20 Desarrollo de las tarifas de Datos Móviles (Velocidades de estándares y tecnologías habilitadoras. Fuente: Jyrki T. J. Pennttinen (2019) [18]

(Ver la Figura 19), las velocidades de estándares y tecnologías como MIMO por fechas y el lanzamiento de la versión 99 de 3GPP, en esta sección incluye MIMO a partir del 2011.

1.5.16 Métodos de Acceso Múltiple entre Generaciones Móviles

En la siguiente tabla de acuerdo con la generación se expresa el tipo de multiplexación que se utilizó su servicio y la banda ancha ideal para funcionar de cada generación.

Tabla 16 Comparación de Métodos de acceso Múltiple entre generaciones. Fuente: Saad Z. Asif (2019) [14].

Gen. Móvil	Forma de onda/ Método de Acceso Múltiple	Aplicación	Banda ancha Canal mínimo	Operación IFFT /FFT
1G	FDMA	Voz	30 kHz	No

2G	FDMA, TDMA CDMA	Voz, baja velocidad Datos alrededor de (100kbps)	200 kHz 1,25 MHz	No
3G	CDMA WCDMA	Voz, velocidad media Datos (aprox. 10s de Mbps)	1,25 MHz 5 MHz	No
4G	OFDMA SC-FDMA	Datos de alta velocidad Móvil Banda ancha Aprox. 100s de Mbps.	1,4 a 20 mHz	Si
5G	Basado en OFDM (Ortogonal) (No Ortogonal) Intercalador / Basado en codificador	eMBB URLLC mMTC	100 de MHz	Si No Si (multipor-tadora)

FDMA es un “Número fijo de usuarios puede acceder al sistema simultáneamente.” [11]

FDMA utilizaba frecuencias separadas [20] requería un gran Ancho de Banda para dar servicio a varios usuarios. [20]

1.5.17 Arquitectura completa de Generaciones Móviles

(Examine la Figura 21,) las diferentes arquitecturas de las distintas generaciones móviles desde el 2G hasta la actualidad 5G, que poseen elementos encargados de manejar el tráfico para poder realizar una comunicación.

Tabla 17 Resumen de los componentes de las Arquitecturas de Generaciones Móviles. Fuente: Elaboración propia en base a [12][18][19][30]

Generación Móvil	Estación Base	RAN	Nombre del núcleo	Elementos de la Capa de Núcleo
2G	BTS	GERÁN	Núcleo de Circuito Conmutado (CS)	MGW, MSC, GMSC, SMSC
3G	NB o NodoB	UTRÁN	Núcleo Conmutado por Paquetes (PS)	SGSN, HLR, GGSN
4G	eNB o eNodeB	E-UTRÁN	Núcleo de Paquetes Revolucionado (EPC)	S-GW, P-GW, MME, HSS
5G	gNB	NR	Núcleo 5G (5GC)	UPF, SMF, AMF, NF1, NF2, NFn

1.5.17.1 2G

Para la arquitectura 2G utiliza la Red de Acceso de Radio Terrestre GERÁN, estructurado por la combinación entre GSM y Edge, una Antena principal llamada BTS dentro de la RAN GERÁN, que es la Estación Base 2G. Para que la Estación Móvil pueda acceder a los servicios que ofrece, tiene que realizar una búsqueda de Estación Base más cercano, este contiene un controlador llamado BSC que se encarga de rotar el tráfico correspondiente.

Utiliza PCU, Unidad de Controlador de Paquetes, más adelante ser conectado al SGSN que se encuentra en el Núcleo Conmutado por Paquetes de la generación 3G, nodo compatible con GRPS. [19] El controlador BSC de la Estación Base utilizada, al enviar la señal desde la

Interfaz de Radio RAN al Núcleo 2G llamado “Núcleo de Circuito Conmutado (CS)” la lleva a la Puerta de Enlace Sede Medios MGW y lo conecta al GMSC, Centro de Conmutación Móvil del Gateway donde se administran las señales. [19] Automáticamente se realiza el enlace con el SMSC, para acceder al servicio de mensajería.

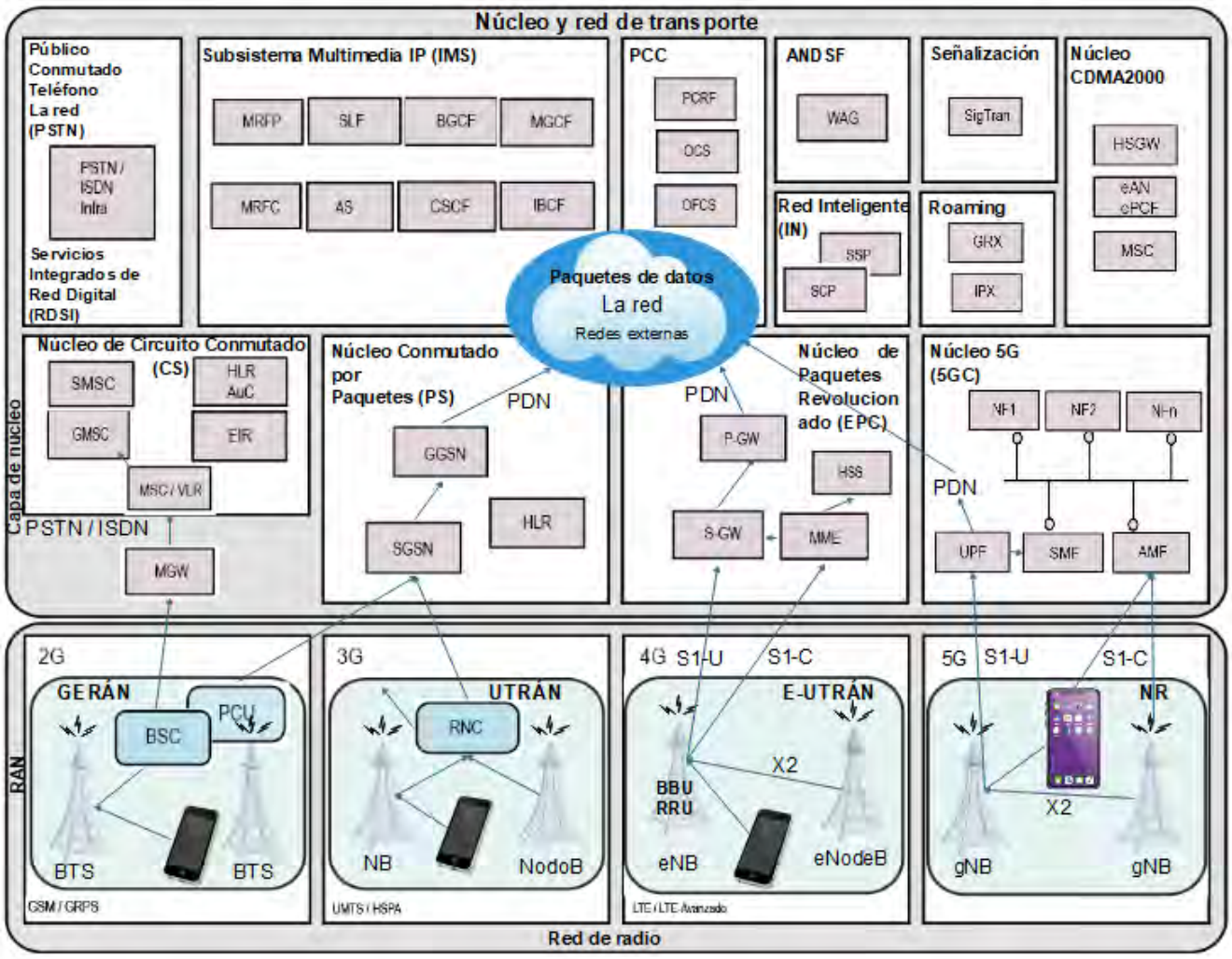


Figura 21 La evolución de la Red Móvil y los elementos de apoyo. Fuente: Jyrki T. J. Penttinen (2019) [18] y apuntes en base a [12][30]

1.5.17.2 3G

3G contiene UTRAN (Red de Acceso de Radio Terrestre Universal) desde el Nodo B o NB que es una Estación Base 3G, Antena principal que administra la señal. [19] Los elementos que hacen posible la comunicación es RNC, elemento de la RAM responsable de controlar el NB y conectar la RAN 3G al Núcleo 3G llamado: “ Núcleo Conmutado por Paquetes (PS).”

Dentro del PS se encuentra SGSN nodo de compatibilidad con GRPS, hace una comunicación con el nodo GGSN que ofrece compatibilidad con GRPS y utiliza la Interfaz PDN para obtener acceso a Internet o algún servicio específico. [19][20]

1.5.17.3 4G

E-Utrán (Evolved-Utran) bajo el nombre de LTE (Long Term Evolution) proporciona Telefonía IP. [19]

La Red de Acceso E-UTRÁN 4G LTE, está presente aún en el 2021 ya que continúa evolucionando, siendo un componente importante en el Acceso de Radio 5G. Esta se compone Estaciones Base llamados eNB o eNodeB, nodo B evolucionado para 4G.

El Equipo del Usuario, en este caso, la Estación Móvil. Por ejemplo para acceder a Internet o una serie de datos, [20] la Estación Móvil escanea entre varios eNB cuál es el más cercano, automáticamente al encontrarlo selecciona la antena de la Celda a utilizar y lo monitorea [11]. La eNB envía la señal del equipo del usuario a la Capa de Núcleo 4G, es decir, el Núcleo de Paquetes Revolucionario (EPC), dónde se encuentran ciertos elementos.

Estos elementos de dividen en dos partes:

- Plano de Usuario que manejan el tráfico de datos: S-GW y P-GW.
- Plano de Control, el MME y HSS.

La Red Central se encarga de realizar la división entre los dos planos [30]

S-GW es el servidor Gateway[19] y P-GW la Puerta de Enlace de Red de paquetes de datos, [20] este controla los servicios de datos IP incluido el enrutamiento la asignación de direcciones IP aplicaciones de políticas y proporciona acceso que no es 3GPP. [20] Utiliza PDN Red Pública de Datos que funciona como Interfaz, para que la P-GW se pueda comunicar con La Red. Así como otros elementos; MME y HSS que pertenecen al Plano de Control.

- MME ese nodo de señalización principal y es responsable de iniciar la búsqueda y autenticación de la estación móvil [17], debido a la movilidad de los usuarios.
- HSS es el servidor abonado doméstico [19] se encarga de autenticar al usuario, autorizar el acceso y cifrar las comunicaciones. [18]

- X2 es la Interfaz que se establece entre una eNB y otra eNB, cuando un usuario está escaneando entre varios eNB cuál es el más cercano, las eNB se comunican entre sí. [19]

Para más información puede verificar el tema: " Definición de Sistema Celular" de la página 12 - 13 , "Organización Celular" de la página 16 – 18, "Pasos de una llamada típica" del Capítulo 1 que se encuentra en la página 19 - 22, "Red de Acceso Radio RAN" de la página 84 - 88, 91 – 96, "Red Central" de la página 88 - 89 del Capítulo 2 y diversos conceptos que se encuentran en la sección "Glosario" 242, así como los Acrónimos.

Entre otros elementos que conforman la Red de Núcleo y de transporte de las distintas generaciones móviles *véase Figura 20*, tenemos como ejemplo:

Tabla 18 Subsistemas multimedia IP (IMS). Fuente: Elaboración propia basado en [18][19].

Subsistemas multimedia IP (IMS)	
MRFP	Se usa para el manejo de dato de usuario en el IMS como grabación y reproducción de voz. [19]
SLF	Base de datos, ofrece a AS por ejemplo la posibilidad de terminar la dirección del HSS responsable de un usuario en específico [19] Función de localización de suscripciones. [19]
BGCF	Funcion de control de puerta de enlace de ruptura[19] decide donde salir de la PSTN si es necesario, recibe la solicitud SIP de CSCF cuando se conecta a una Red de conmutación de circuitos.
MGCF	Funcion de control de puerta de enlace multimedia. [19]
MRFC	Controlador de funciones de recursos multimedia. [19] Para el control de procesamiento de los datos de los usuarios.
AS	Servidor de aplicaciones. [19]
CSCF	Función de control de sesión de llamada [19] consulta el HSS durante el registro para el S-CSF responsable que funciona como un servidor proxy SIP.

IBCF	Funcion de control de fronteras de interconexión. [18]

Los conceptos restantes que se encuentra en la Figura 21, los puedes encontrar en "Glosario" que se encuentra al final del documento.

(Examine la Figura 22,) las divisiones entre la RAN, la Red Principal y los elementos que lo conforman de las distintas generaciones móviles.

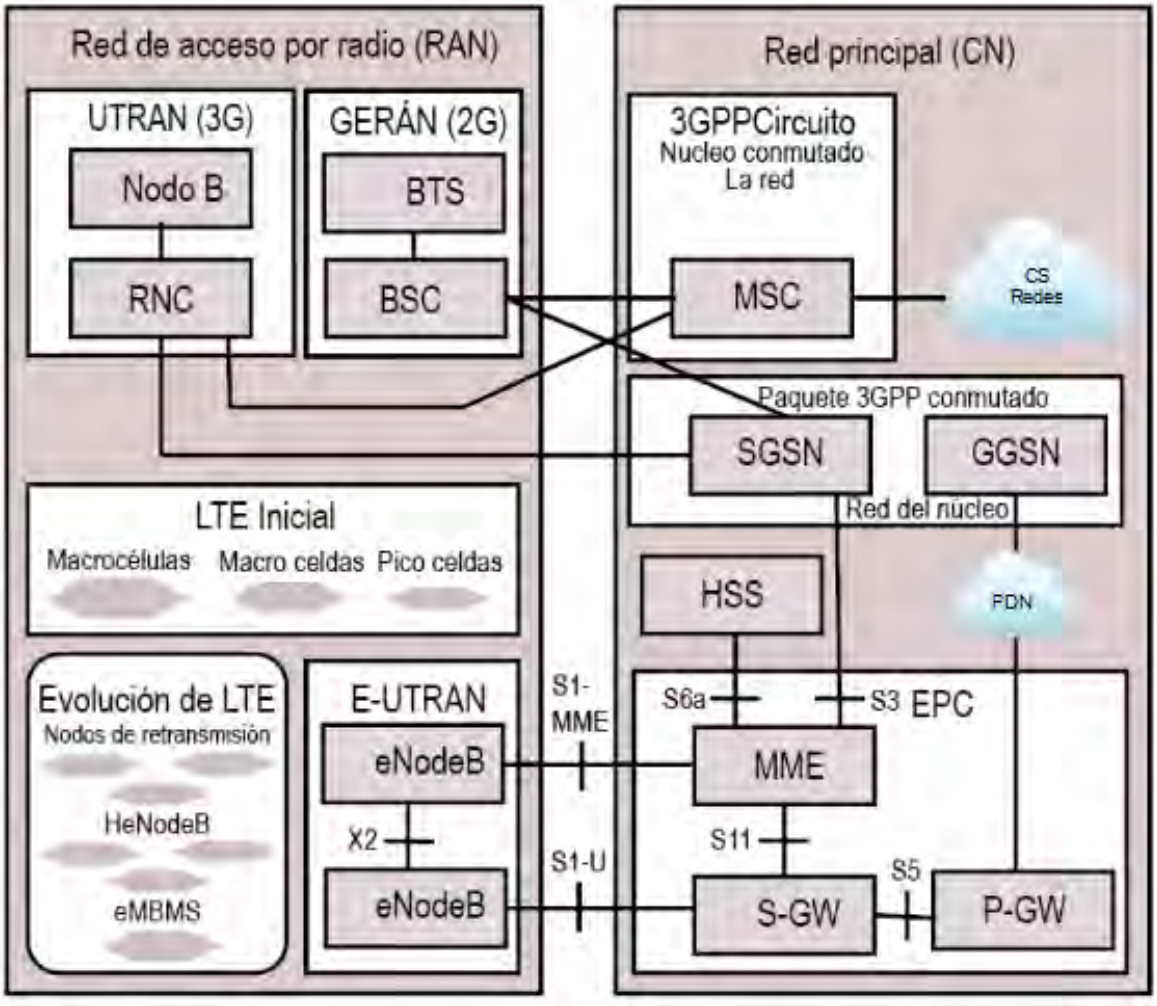


Figura 22 Los elementos clave de la arquitectura de Red 2G, 3G, 4G antes de la implementación de 5G. Fuente: Jyrki T. J. Penttinen (2019) [18]

1.5.18 Arquitectura LTE

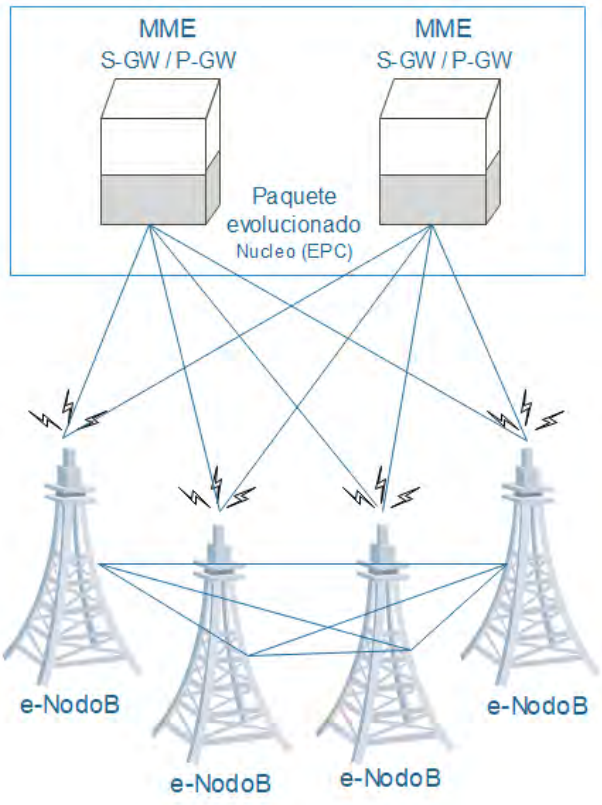


Figura 23 Arquitectura LTE. Fuente Madhusanka Livanage (2018) [20]

(Ver la Figura 23.) El nodo B se conoce como eNodoB, cada nodo está conectado a la EPC una Red central plana basada en IP, (se puede acceder a través del acceso por Radio 3GPP), combinación entre S-GW servidor Gateway y puerta de enlace de Red de paquete de datos.

P-GW “controla los servicios de datos IP incluido el enrutamiento, asignación de direcciones IP, aplicación de políticas, etc.” [20] MMM es la entidad de gestión de la movilidad, su función es autenticar al usuario para que pueda acceder a un servicio en particular. [20]

1.5.19 Evolución de Amenazas y Seguridad en Generaciones Móviles

El avance de la tecnología móvil ha permitido alcanzar grandes expectativas en los últimos años, mejoras en cada generación, pero además de los beneficios que han ofrecido,

ha sido vulnerable a distintas amenazas que ponen en riesgo la Seguridad del usuario. Mantener la Red segura y los equipos ha demostrado que reduce efectos negativos ante el uso de esta plataforma (véase Figura 24). [20]

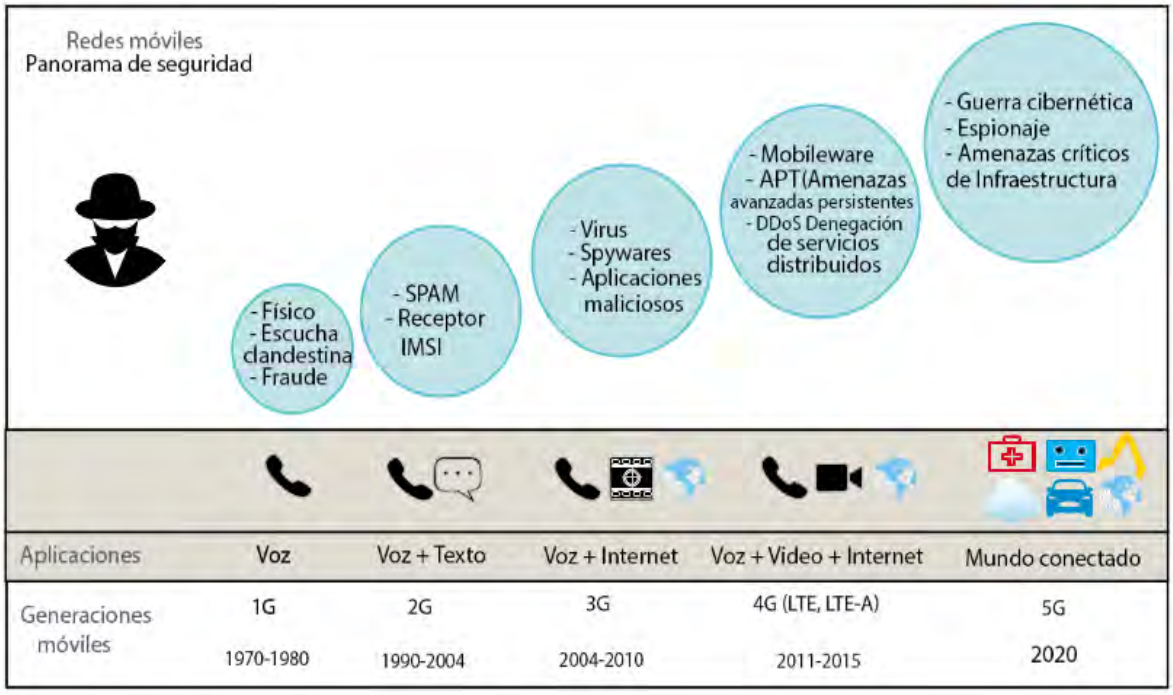


Figura 24 Panorama de la Seguridad de la red móvil. Fuente: Madhusanka Livanage (2018) [20]

En esta sección tenemos las distintas generaciones móviles que han formado parte de nuestra vida diaria, las amenazas de Seguridad que han presentado y los métodos de Seguridad implementados para mitigar los riesgos. [20]

1.5.19.1 1G Primera Generación Móvil

Tabla 19 Amenazas y Seguridad específicas para la Primera Generación Móvil. Fuente: Elaboración propia basado en Madhusanka Livanage (2018) [20]

Generación	Vulnerabilidad	Amenazas de Seguridad	Riesgo	Seguridad
1G	Sin confidencialidad en la	Escucha de comunicación privada entre dos usuarios. [20]	Variable. [20]	No contaba con seguridad. [20]

(Primera Generación)	comunicación. [20] Sin mecanismos de identificación o autenticación integrados para identificar de forma única el usuario. [20]	Clonación de identidad de manera fácil en teléfonos móviles. [20] Venta de teléfonos clonados ilegales. [20]	Los cargos de llamadas realizadas se dirigían al propietario original. [20] Secuestro de canales, escuchas clandestinas. [20]	Existió intento de mitigar la clonación masiva, no fue un éxito. [20]

Figura 25 Ataque de clonación de teléfonos celulares en la Red 1G. Fuente: Madhusanka Livanage (2018) [20]

Como se muestra en la (Figura 25) de ejemplo, un atacante interfiere en la comunicación entre la Estación Base y el Móvil de usuario haciéndose pasar por un suscriptor legal para realizar llamadas gratuitas, esto mediante un radio receptor, clona la información de identidad móvil que es el número del móvil de usuario y su ESN utilizando un pc con

software. Los atacantes pueden utilizar diversas herramientas como Oki 900 y así realizar llamadas gratuitas. [20]

1.5.19.2 2G Segunda Generación Móvil

Tabla 20 Amenazas y Seguridad específicas para la Segunda Generación Móvil. Fuente: Elaboración propia basado en Madhusanka Livanage (2018) [20]

Generación	Vulnerabilidad	Amenazas de Seguridad	Riesgo	Seguridad
2G Segunda Generación móvil.	Mensajes. [20] Creación de estaciones base no autorizado [20] (IMSI Catchers)	Spam. [12] Autenticación de red falsa. [20]	Saturación de almacenamiento en el equipo. [20] Información falsa. [20] Intercepción del tráfico móvil. [20]	Protección de cifrado básica para señalización y datos de usuario. [20]

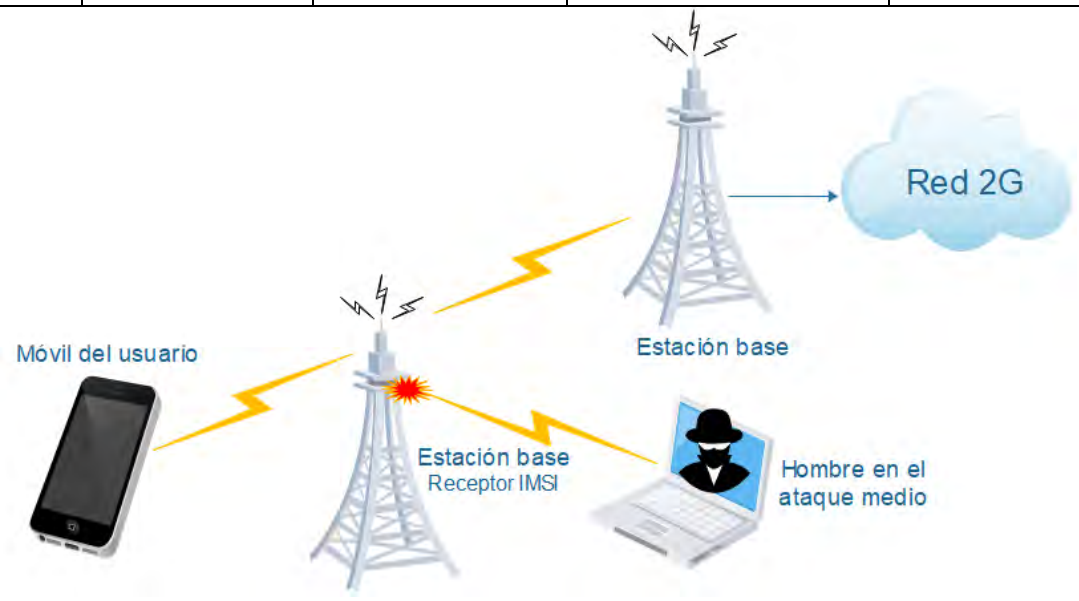


Figura 26 Ataque IMSI Catcher en Red 2G. Fuente: Madhusanka Livanage (2018) [20]

Mientras intentaban mitigar los ataques de la primera generación con la autenticación de usuarios por medio del módulo de identidad del suscriptor (SIM) como identificación única de usuario, surgió una nueva amenaza, el hombre de en medio o ataque intermediario (MitM), utilizando estaciones base no autorizados llamados IMSI Catcher permitiendo que los usuarios se conecten a canales no seguros, otra manera de interferir en la comunicación (ver Figura 26). [20]

1.5.19.2.1 Seguridad en GSM

GSM se centra en cuatro aspectos importantes, de los cuáles las medidas de Seguridad a implementar son: [20]

Tabla 21 Amenazas y Seguridad en estándar GSM de Segunda Generación Móvil. Fuente: Madhusanka Livanage (2018) [20]

Aspectos de Seguridad por tratar	Seguridad
Uso de módulo de identidad del suscriptor (SIM) y Autenticación de usuario. [20] Cifrado de datos y señalización. [20] Confidencialidad de la identidad del usuario. [20]	Uso de SIM para autenticarse y demostrar que el usuario es cliente legítimo que solicita el servicio de un operador en particular. [20] Encriptación de datos y la señal. [20] • Uso de IMSI. [20] • Ki. [20] • Algoritmo A3, A8, A5. [20]

1.5.19.2.1.1 SIM

La SIM según Madhusanka Liyanage (2018) “es básicamente una tarjeta inteligente desmontable que contiene información del suscriptor y se utiliza para probar su identidad con el operador junto la información sobre los tipos de servicios que se les permite acceder.” [20]

1.5.19.2.1.2 IMSI

IMSI (Identidad de suscripción móvil internacional) “representa el número único para cada suscriptor del mundo y lleva información sobre la Red doméstica del suscriptor y el país al que pertenece.” [20] Se compone de 15 decimales, los primeros 5 dígitos son asignados a la Red y el país de origen. Esta información contiene una clave de cifrado llamado Ki, A3 un algoritmo que proporciona autenticación del usuario para acceder al sistema, A8 para proteger los datos y la señalización, A5 el cifrado de flujo de datos. *Para más información en el tema: “Seguridad en GSM” puede consultar el libro de referencia n. 12 “A comprehensive Guide to 5G Security” del 2018 en la página 11- 14. [20]*

1.5.19.3 3G Tercera Generación Móvil

“3G decidió basar su Seguridad siguiendo el marco CIA (Confidencialidad, Integridad y Disponibilidad). Como resultado, se adoptó el protocolo AKA (Autenticación y acuerdo de claves) para la autenticación bidireccional entre el equipo del usuario y la Red.” [20]

1.5.19.3.1 Seguridad en CDMA2000

El estándar CDMA2000 de 3G para ofrecer Seguridad incluyó las siguientes entidades: Red doméstica, el Centro de Autenticación, Registro de Ubicación Doméstica (HLR/AC), la Red de Servicio, el Registro de Ubicación de Visitantes, el Controlador de la Estación Móvil / Nodo de Servicio de Paquetes de Datos (VLR y MSC / PDSN), el Abonado Móvil (MS) y el Módulo de Identidad de Usuario (UIM). [20]

Tabla 22 Amenazas y Seguridad específicas para la Tercera Generación Móvil. Fuente: Elaboración propia, basado en Madhusanka Livanage (2018) [20]

Generación	Vulnerabilidad	Amenazas de Seguridad	Riesgo	Seguridad

3G Tercera Generación	Aplicaciones de datos e Internet. [20] Reemplazo de dispositivos móviles por teléfonos inteligentes. [20] Instalación de aplicaciones no autorizadas. [20]	Integración de código malicioso en forma de Malware y Spyware. [12] Sistema operativo. [20]	Acceso no autorizado a información personal confidencial como contraseñas o contactos. [20] Vulnerable a filtrado de datos, virus, Spyware. [20] Teléfonos pirateados. [20] Degradación del rendimiento de los servicios proporcionados. [20]	IMT-2000 proporcionó un estándar para las aplicaciones de todo el mundo. [20] Parches y actualizaciones regulares de Seguridad. [20] Implementación de políticas de Seguridad de aplicaciones estricta. [20]

1.5.19.3.2 Seguridad en UTMS

El estándar UTMS ofreció Seguridad en:

1.5.19.3.2.1 Acceso a la Red

"Proporciona al suscriptor acceso seguro a los servicios 3G y brinda protección contra ataques a la Interfaz de Radio." [20]

1.5.19.3.2.2 Autenticación de usuario

“Es propiedad de la red que presta el servicio confirmando la validez de la identidad del usuario.” [20]

1.5.19.3.2.3 Autenticación de la Red

“Es la propiedad que el usuario valida, que está conectada a una Red de servicio y está autorizada por la Red doméstica del usuario.” [20]

1.5.19.3.2.4 Dominio de Red

“Permite que todos los suscriptores puedan intercambiar datos de señalización de forma segura y proporciona protección contra ataques a la Red fija.” [20]

1.5.19.3.2.5 Dominio del usuario

“Encargado en el acceso seguro de las Estaciones Móviles.” [20]

1.5.19.3.2.6 Dominio de la aplicación

“Asegura de que las aplicaciones en el dominio del usuario y del proveedor puedan comunicarse entre sí de forma segura.” [20]

1.5.19.4 LTE

Tabla 23 Amenazas y Seguridad específicas para LTE. Fuente: Madhusanka Livanage (2018) [20]

	Vulnerabilidad	Amenazas de Seguridad	Riesgo	Seguridad
LTE Long Term Evolution	E-UTRAN LTE. [20]	Explotación de Red de núcleo LTE con identificador temporal. [20]	Obtener el acceso a ubicaciones de Equipo de usuario. [20]	“Cifrando la señal de control de tráfico y los mensajes de comando.” [20]

1.5.19.5 4G Cuarta Generación Móvil

Tabla 24 Amenazas y Seguridad específicas para la Cuarta Generación Móvil. Fuente: Madhusanka Livanage (2018) [20]

Generación	Amenazas de Seguridad	Seguridad
4G Cuarta Generación	S.O inseguro. [20]	Sistema operativo parchado y actualizado. [20]
	Descargar aplicaciones no autorizadas. [20]	Instalación de aplicaciones autorizadas en los dispositivos móviles. [20]
	Virus. [20]	Instalación de antivirus. [20]
	Software malicioso [20]	Descarga de aplicaciones sólo en la tienda de aplicaciones del proveedor. [20]
	Software espía. [20]	Definir una política de acceso al servicio de cada aplicación. [20]
	DDos (Denegación de Servicio Distribuido). [20]	Habilitar el cifrado en dispositivos móviles. [20]

Capítulo 2: 5G

2.1 Introducción

Con el pasar del tiempo, las Generaciones Móviles del uno al cuatro han evolucionado con grandes cambios en su tiempo, pero debido a la gran demanda de usuarios conectados que surge cada día, el incremento de los diferentes tipos de tráfico en la utilización de los equipos móviles, generan limitaciones de rendimiento del sistema y nuevas necesidades por satisfacer.

Es por eso, que sea ha requerido el desarrollo de una nueva Generación Móvil, más sofisticado, dirigido a una gran variedad de diferentes tipos de usuario y conexión, funciones IoT, ya que cuenta con una gran escala de capacidades y servicios que ofrecer, pero también esos desarrollos innovadores han generado riesgos significativos que amenazan la Seguridad de los usuarios, siendo objeto adherente de sus vulnerabilidades.

En este capítulo nos centraremos en las Redes 5G como una transformación más allá de las Redes de telecomunicaciones móviles convencionales, sus principales componentes, características y los riesgos que suponen, el análisis general entre los riesgos, medidas de Seguridad y comparativa de Seguridad entre 4G y 5G (ver Figura 27).

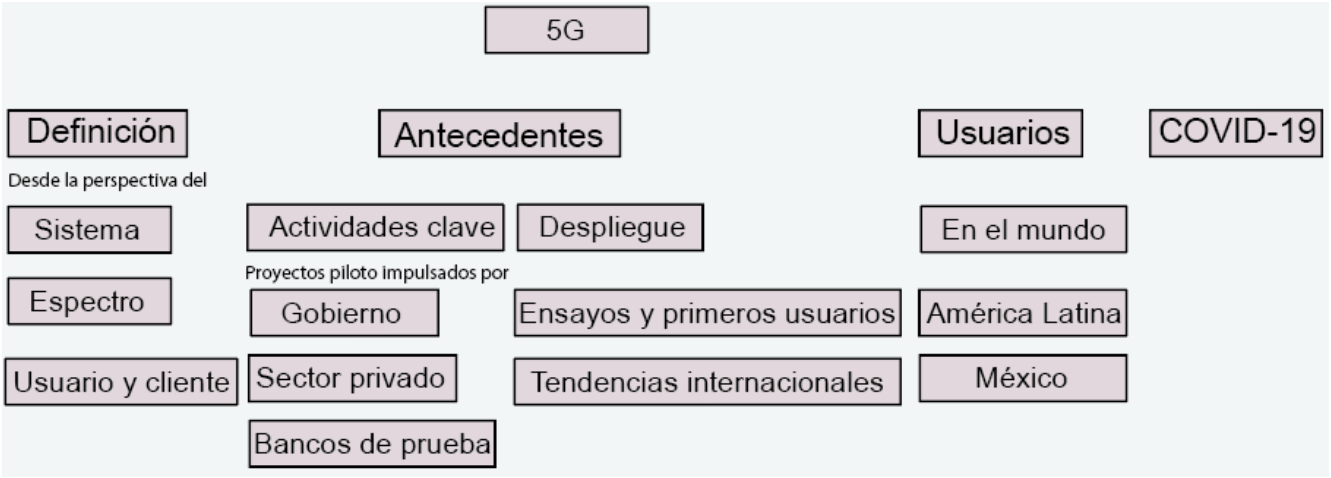


Figura 27 Introducción de la Red 5G. Fuente: Elaboración propia.

2.1.1 Definición 5G

Hay diferentes definiciones para 5G, la Generación Móvil de Quinta Generación.

Según Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) 5G se define de acuerdo con 3 perspectivas;

2.1.1.1 Desde la perspectiva de la arquitectura del sistema

"5G será una combinación de tecnologías de Acceso Múltiple, que incluyen tecnologías de Radio de Acceso actuales y existentes como LTE y New Radio (NR) para 5G, así como la evolución de los paradigmas de Redes emergentes actuales como la Computación en la Nube, las Redes Definidas por Software (SDN) y la Virtualización de Funciones de Red (NFV)." [20]

2.1.1.2 Desde la perspectiva del espectro, es decir, desde el espacio de conexión

"5G asignará una cantidad significativa de espectro nuevo para hacer frente a dispositivos conectados masivamente, redes muy tensas y para admitir una variedad de casos de uso, en lo que las Bandas de Frecuencia tradicionales no podrían proporcionar suficiente Ancho de Banda. La conferencia Mundial de Radiocomunicaciones en Noviembre del 2015 identificó una gama de nuevas Bandas de espectro por debajo de 6 GHz que se pueden utilizar para dispositivos Móviles." [20]

2.1.1.2 Desde la perspectiva del usuario y del cliente

"Con 5G se puede experimentar muchos tipos de servicios recientemente definidos como la Realidad Virtual, Realidad Aumentada para juegos u otros propósitos, videos de alta definición y tridimensionales, conducción autónoma, entre otros." [20]

Según Sassan Ahmadi (2019) "es un conjunto de tecnologías conectado, rápido, seguro y confiable que comprende de humanos y máquinas, lo que permite la movilidad perfecta, conectividad eficiente, una mayor densidad de conexión, aumento en la productividad industrial, automatización y sostenibilidad. Las sociedades conectadas del futuro se caracterizan por el crecimiento significativo de la conectividad y la densidad de tráfico, la densificación de la Red y la amplia gama de nuevos casos de uso y aplicaciones." [24]

La idea de alto nivel de 5G es unir a las personas a través de un conjunto de cosas, datos, aplicaciones, sistemas de transporte y ciudades en un entorno de comunicaciones de Red Inteligente. [18]

El término 5G hasta el 2019 es confuso, [18] pero la definición más actualizada resulta más conveniente.

En conclusión, tenemos que 5G: Es conjunto de tecnologías en una sola estructura que conecta personas con personas y personas con todo. [17] 5G funciona como plataforma para garantizar un desarrollo fluido de IoT y actúa como un facilitador para las comunicaciones inteligentes en Red. [18] "Contiene una nueva tecnología de Acceso por Radio llamado 5G NR (New Radio) y una Red Central mejorada llamada NGC (Next Generation Core)." [14]

"El objetivo del estándar global 5G (3GPP) es proporcionar la interoperabilidad entre redes y dispositivos, ofrecer sistemas seguros y enérgicamente eficientes de alta capacidad y aumentar significativamente las tasas de datos de usuario con mucho menos retraso en el tiempo de respuesta." [18] *Para más información de 3GPP, recapitule tema: "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.*

2.1.2 Antecedentes

5G despertó un gran interés en la industria de telecomunicaciones y se pudo esperar que los gobiernos, el sector privado y el mercado, implementaran 5G como etapa inicial mediante pruebas o actividades, mucho antes de que se presentaran y aprueben formalmente las tecnologías candidatas reales de UIT-R[33] en IMT-2020.[34] [18]

Las actividades 5G comenzaron en el 2013, al menos un par de años antes que el 3GPP y la UIT publicaran formalmente cualquier agenda específica sobre el 5G. [14] *Véase Tabla 25.*

Tabla 25 Actividades clave de 5G. Fuente: Saad Z. Asif (2019) [14]

Año	Ocupaciones
2013	o China formó el grupo de promoción IMT-2020 para promover la infraestructura y el desarrollo de 5G dirigiendo las pruebas del país y otras actividades. Corea del sur formó el Foro 5G para convertirse en la fuerza líder en el desarrollo de la tecnología de comunicación de próxima generación. o Los profesores de la Universidad de Texas en Austin y de la Universidad de Stanford recibieron una subvención de la National Science Foundation (NFS) para investigación de las redes inalámbricas 5G.
2014	o 5G-PPP (Asociación Público - Privada de Infraestructura 5G) es una iniciativa de la Unión Europea del 2014. 5G-PPP seleccionó 19 proyectos durante su Call-1 que comenzó en el segundo trimestre del 2015. o La Unión Europea y Corea del Sur firmaron un Memorando de Entendimiento para colaborar con la armonización de sistemas, estándares y radiofrecuencia 5G. La Alianza NGMN (Next-Generation Mobile Networks) inició en trabajo en 5G.

[33] *Para más información verificar página 30 – 31.*
[34] *Para más información véase de la página 34-36*

2015	o La administración de Estados Unidos lanzó una iniciativa de investigación avanzada de 400 millones de dólares dirigida por la National Science Foundation (NSF). o Inició el Proyecto Clave Nacional de China sobre 5G. o La organización 3GPP inició una nueva fase de estudios para 5G. o Huawei inició una prueba de campo conjunta de las nuevas tecnologías de Acceso por Radio 5G con NTT DoCoMo.
2017	UIT-R publicó los requisitos de rendimiento técnico de las IMT-2020.

E*n la Tabla 25 podemos ver las primeras actividades generales a nivel internacional del 5G.*

2.1.2.1 Proyectos piloto impulsados por los Gobiernos

Para poder fomentar la inversión de redes e infraestructura 5G, se puso en marcha los proyectos tecnológicos impulsados por gobiernos desde sus fases tempranas: [21]

Podemos ver en la Tabla 26 los proyectos piloto desde sus inicios impulsados por los gobiernos de diferentes países.

2.1.2.2 Bancos de prueba 5G impulsados por el Sector Privado

"Además, el sector de las telecomunicaciones, incluidos operadores, vendedores y Centros de Investigación, han participado en Bancos de Pruebas independientes de los gobiernos. [21] *Examine la Tabla 27.*

Tabla 26 Iniciativas 5G impulsadas por gobiernos. Fuente: UIT(2018)[21]

El Gobierno de Corea (Rep. de), a través de la NISA, instaló redes piloto 5G durante los Juegos Olímpicos de Invierno de 2018, gracias a las cuales brindó experiencias futuristas como la navegación basada en la realidad aumentada, [21] basado en bandas mmWave (milimétricas). [18]
Se ha concedido una subvención pública de 17,6 millones de libras esterlinas a un consorcio dirigido por la Universidad de Warwick, con miras a la creación de un Banco Central de Pruebas para Vehículos Autónomos Conectados (VAC) en el Reino Unido. En este caso, se instalarán Células pequeñas a lo largo de una carretera que atraviesa Coventry y Birmingham, en la que se pondrán a prueba los VAC.
La FCC (EE.UU.) ha alentado a la comunidad investigadora a presentar solicitudes de obtención de licencias experimentales para radiofrecuencias no concedidas o asignadas, a fin de promover la innovación y la investigación a través de experimentos en zonas geográficas definidas.
El programa de trabajo Horizonte 2020 de la CE (2018-2020) fomenta la innovación en materia de 5G con la participación de la UE (Unión Europea), China, Taiwán y los Estados Unidos. Entre las actividades realizadas figuran pruebas de extremo a extremo relacionadas con la movilidad conectada y automatizada transfronteriza, así como pruebas de 5G en múltiples industrias verticales.
La Unión Federal de Instalaciones de Investigación en Telecomunicaciones para un Laboratorio Abierto UE-Brasil (FUTEBOL) ha puesto en marcha una investigación encaminada a la Promoción de Recursos de Telecomunicaciones Experimentales en Brasil y Europa. FUTEBOL también demostrará casos de uso basados en IoT, redes heterogéneas y C-RAN.
El Ministerio de Comunicaciones de la Federación de Rusia suscribió un acuerdo con Rostelecom y Tattelecom, con el objetivo de crear una zona 5G experimental en la tecnológica ciudad de Innopolis.

Tabla 27 Bancos de Prueba 5G impulsados por el sector privado. Fuente: UIT(2018)[21]

Telstra (Australia) está colaborando con Ericsson en el desarrollo tecnologías 5G fundamentales, entre ellas, MIMO Masivo, Formación de Haces, Seguimiento de Haces

y Formas de Onda. Durante la primera prueba de 5G en directo realizada en Australia, Telstra y Ericsson alcanzaron velocidades de descarga de entre 18 Gbit/s y 22 Gbit/s. Optus también completó una prueba de 5G con Huawei, en cuyo marco se alcanzó la mayor velocidad registrada en Australia hasta este momento, a saber, 35 Gbit/s.
El operador móvil italiano Wind Tre, Open Fibre (operador mayorista italiano de fibra) y el proveedor chino ZTE han anunciado la creación de una asociación para construir lo que, según ellos, será la primera Red precomercial 5G de Europa en la banda 3,6- 3,8 GHz. También colaborarán con universidades, centros de investigación y empresas locales para probar y verificar el rendimiento técnico de la 5G, la arquitectura de la Red, la integración de la Red 4G/5G y los futuros casos de uso de la 5G, incluidas la Realidad Virtual o Aumentada, las Ciudades Inteligentes, la Seguridad Pública y la Asistencia Sanitaria 5G. El proyecto piloto concluirá en Diciembre de 2021.
En el marco de un proyecto liderado por MegaFon, se procedió a la instalación una Red piloto 5G en el interior y los alrededores del estadio Kazan Arena (Federación de Rusia) con ocasión de la Copa del Mundo de fútbol de 2018. Rostelecom también está trabajando con Nokia en una red inalámbrica 5G piloto, ubicada en un parque empresarial de Moscú, a fin de poner a prueba diversos casos de uso de la 5G.
Verizon (EE.UU.) anunció que estaba proyectando una serie de pruebas 5G en varias ciudades estadounidenses. Las instalaciones funcionarán con enlaces de conexión al núcleo de Red inalámbricos en lugar de por fibra. AT&T también indicó que realizaría pruebas comerciales de tecnología inalámbrica fija 5G, basadas en los últimos experimentos que llevó a cabo en Austin, donde alcanzó velocidades de 1 Gbit/s y una latencia inferior a 10 milisegundos. Las pruebas se efectuarán con equipos de Ericsson, Samsung, Nokia e Intel.
Comsol ha previsto lanzar la primera Red inalámbrica 5G de Sudáfrica. Los experimentos de Comsol pondrán a prueba la calidad de funcionamiento de la 5G en condiciones reales, utilizando soluciones de Células Pequeñas y Macrocélulas. Es probable que Comsol ofrezca servicios inalámbricos fijos frente a los servicios de fibra hasta el hogar (FTTH).
Huawei y NTT DOCOMO alcanzaron una velocidad de descarga de 4,52 Gbit/s en 1,2 km. Huawei aportó una Estación Base 5G, que soporta tecnologías de MIMO Masivo y Formación de Haces, además de su Red Básica 5G.

2.1.3 Despliegue

"Los despliegues iniciales de 5G operarán en una Red no dependiente (NSA), en otras palabras, operarán en la infraestructura 4G y 4G-LTE existente y en las infraestructuras híbridas 4G/5G independientes, probablemente en dos años." [25][26]

2.1.3.1 Ensayos y primeros usuarios antes del 2020

La evolución completa de las capacidades de la Red 5G todavía está en desarrollo, ya que tiene como objetivo hasta ahora cumplir con los crecientes requisitos de datos y comunicación, incluido la capacidad de conexión de millones de usuarios, la limitación que tiene en zonas urbanas, entre otros. [18][25]

Entre los mercados interesados que implementaron 5G antes del 2020 ya mencionados han sido:

2.1.3.1.1 Verizon Wireless

Además de la configuración cooperativa con Samsung, Nokia e Intel, ha trabajado con Cisco, Qualcomm para poder definir una plataforma común y ampliable para las pruebas e implementaciones en conjunto de acceso inalámbrico fijo de 28 y 39 GHz. El objetivo principal de sus ensayos en general ha sido recopilar experiencias sobre el rendimiento esperado del 5G final. [18]

2.1.3.1.2 AT&T

Juntamente con Ericsson, Samsung, Nokia e Intel, en Estados Unidos. Teniendo como objetivo la obtención de información sobre el rendimiento y la propagación de ondas milimétricas, la ubicación de los dispositivos, la topología e impactos climáticos en el enlace de Radio. [18]

2.1.3.1.3 DoComo

DoComo ha estado activo en las pruebas de concepto 5G en Tokio, mediante bandas y velocidades de datos en tales bandas, implementando conocimientos aplicados sobre las especificaciones de 3GPP 5G NR como una nueva Red de acceso por Radio, juntamente con NTT DOCOMO. Los resultados de las pruebas ha sido la mejora de rendimiento máximo de 1Gb/s apto para videoconferencia en tiempo real por cada usuario. [18]

2.1.3.2 Tendencias Internacionales

2.1.3.2.1 OCDE

La OCDE es la Organización para la Cooperación y el Desarrollo Económico, fue fundada en 1961 con el propósito de promover políticas que mejoren el bienestar económico y social de las personas de todo el mundo. OCDE ofrece un foro donde juntamente con los gobiernos de 36 países analizan y comparan datos para realizar pronósticos de tendencias, buscan soluciones de problemas comunes, miden en conjunto la productividad y los flujos globales del comercio e inversión. [22]

En octubre del 2018, la OCDE publicó el documento “The road to 5G Networks Experience to Date and Future Developments” desde la perspectiva de “Estrategias Nacionales 5G” documento generado a partir de discusiones dentro del foro como la infraestructura 5G, la implementación de las primeras pruebas impulsados por los países involucrados, problemas que puedan surgir en:

- La gestión y planificación del espectro radioeléctrico.
- Calidad de Servicio y derechos de usuario.
- La regulación orientada a la Seguridad y privacidad de los usuarios en los servicios y aplicaciones que ofrece. [22]

Algunos países que pertenecen a la OCDE tenemos: la Unión Europea, Reino Unido, Alemania, Estados Unidos, Brasil, Chile, México, entre otros. [22]

2.1.4 Usuarios de Telefonía Móvil y 5G

2.1.4.1 En el mundo

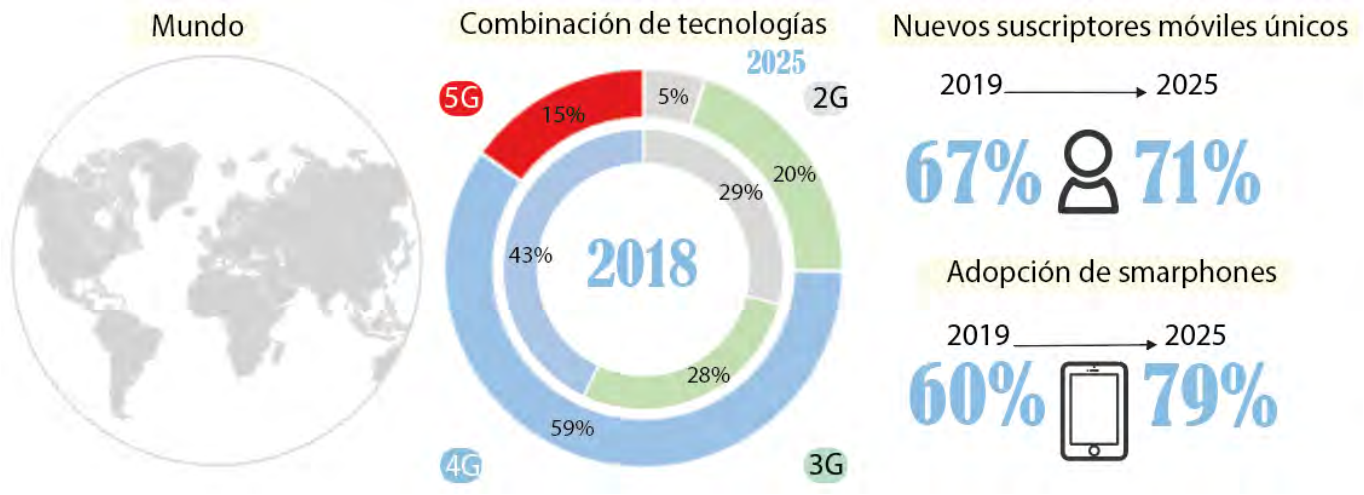


Figura 28 Suscriptores 5G en el mundo. Fuente: Plan 5G Colombia (2019)[22]

En el mundo todavía existe la conexión híbrida de usuarios que usan 2G, 3G y 4G. Si consideramos como referencia el 2018, el 29% de conexiones era para 2G, 3G con el 28% y 4G con el 43%, se estima que para el 2025 las conexiones 2G se reduzcan al 5%, 3G disminuya al 20%, 4G incremente al 59% y 5G alcance el 15% de usuarios conectados en el mundo (*ver la Figura 28)*. [22]

2.1.4.2 América Latina

Existe una gran demanda de usuarios conectados cada día, en América Latina por ejemplo, ha llegado a finales del 2020 con 440 millones de suscriptores móviles únicos, 500 millones de conexiones de smartphones para el 2023, más de 400 millones de suscriptores a Internet móvil para el 2025. Sin embargo aproximadamente 300 millones de personas en la región todavía no se pueden conectar al Internet móvil por diversos motivos como puede ser falta de recursos económicos, la edad, el sexo, siendo las mujeres con menor tasa de participación. [27]

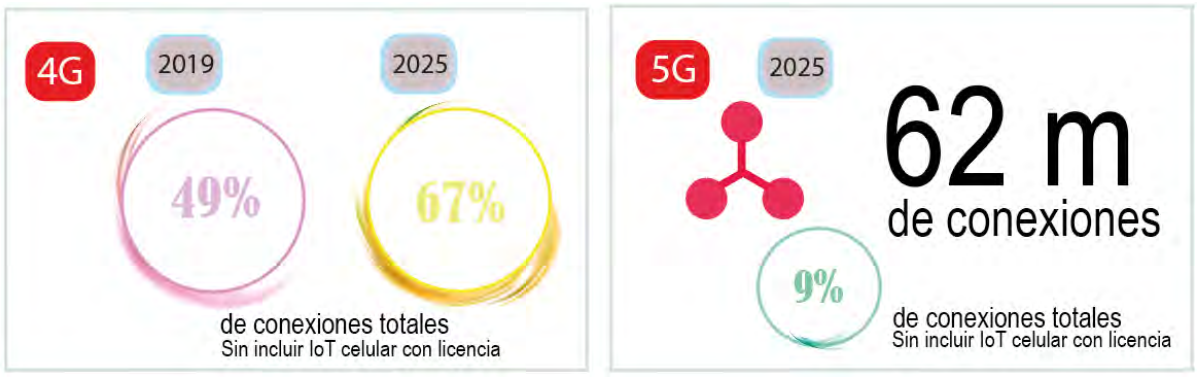


Figura 29 Comparativa entre conexiones totales por año del 4G y 5G. Fuente: GSMA (2020)[27]

Aun así, se espera 15 millones de conexiones 5G en el 2022, 62 millones para el 2025, siendo el 9% de conexiones totales sin incluir IoT ya que todavía no ha tenido una evolución significativa, a comparación del 4G que sigue vigente, en el 2019 ha tenido el 49% de conexiones totales sin incluir IoT y en espera del 67% para el 2025 (v*éase Figura 29)*. [27]

2.1.4.3 México

Hasta el 2019 la Red 3G ha predominado con el 56% de usuarios, una minoría del 13% para la 2G, y el 31% para 4G, esto se debe que aproximadamente en el 2019 se ha tenido el 63% de nuevos suscriptores móviles únicos, esperando que para el 2025 alcance el 70%, pero a pesar de esto, no todas las personas cuentan con recursos económicos o suponen que no necesitan un teléfono móvil para su vida cotidiana. La adopción de smartphones o telefonía móvil en el 2019 ha sido del 65%. [27]

Se considera que para el 2025 4G sea la Red predominante con un 55%, reduciendo al 2% 2G y 3G con el 31%, iniciando el despliegue 5G con un 12%.[27] *Véase la Figura 30 la representación del uso de las redes 2G - 4G en México, el porcentaje de nuevos suscriptores y la adopción de smartphones.*

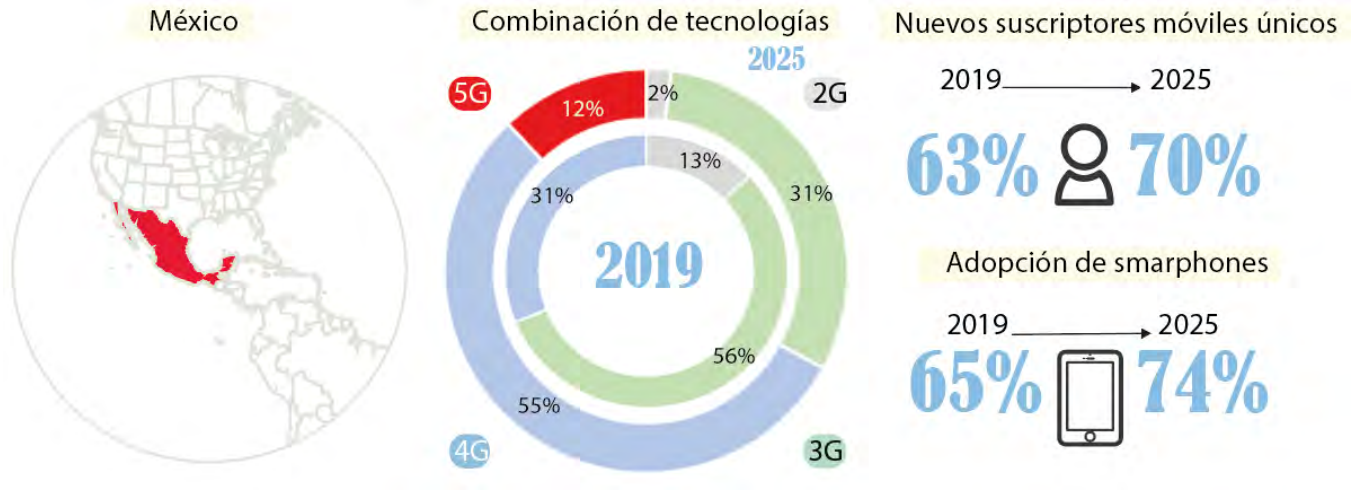


Figura 30 Tendencias tecnológica y suscriptores para mercados clave en México. Fuente: GSMA (2020)[27]

2.1.5 5G y Covid-19

Esto quiere decir que ha existido un retraso de despliegue 5G en América Latina, inclusive en el mundo y se debe a la pandemia COVID-19. [27] Por ejemplo:

- Suecia y Sudáfrica implementaron 5G de manera temprana para asegurar la capacidad disponible suficiente durante la crisis. [27]
- India pospuso la implementación hasta el 2021. [27]
- Grecia y Portugal informaron interrupciones en las implementaciones de 5G. [27]
- 45 operadoras lanzaron servicios 5G comerciales durante los nueve meses del 2020. [27]
- “La era de la tecnología 5G comenzó en América Latina con el lanzamiento de servicios 5G en Brasil y Uruguay en 2020. Para la primera mitad de 2021 se esperan subastas de las bandas de espectro de 3.5 GHz y 26 GHz en Brasil, y los reguladores en Chile, Colombia y República Dominicana han anunciado sus intenciones de asignar espectro 5G en este 2021.” [27] “Asegurar que los recursos de espectro necesarios estén disponibles en óptimas condiciones en el momento de lanzamiento oportuno, ayuda a reducir los costos de banda ancha móvil” ya que la cantidad de nuevo espectro móvil determinará el éxito de los servicios 5G. [27]
- México.

La pandemia también ha causado un impacto económico en la vida de los consumidores. La mitad de los consumidores mediante encuestas hechas por GSMA, afirmaron la reducción de sus ingresos, siendo cautelosos en la compra de dispositivos [28], ya que fueron calificados como compras no esenciales. [27]

En mayo del 2019, antes de crisis sanitaria los usuarios de telefonía estaban dispuestos a realizar la transición del 4G a 5G pagando una prima del 20% por un plan 5G incluido tres servicios digitales de su elección, pero a causa de la pandemia, la reducción de ingresos, las prioridades en salud y alimentación debido al aislamiento que se suscitó, la caída económica ya no era posible contar con ese recurso, por lo cual solamente podían pagar en promedio un 10%. [28]

Asimismo, el 25% de los consumidores han dicho que existe la probabilidad de actualizarse a un teléfono smartphone compatible con 5G, de esta cantidad, el 16% no lo había planeado, pero está en proceso de actualizarse ya sea por la presión social, la novedad o simplemente cree que los requisitos que ofrece 5G será de su beneficio en la vida profesional y cotidiana. [28]

Quienes ya cuentan con IPhone, por ejemplo la versión 12 y 13 son compatibles con la Red 5G, aunque no cuenta con una cobertura amplia en ciertas áreas. [29] En Estados Unidos, Australia, Suecia y Suiza, usuarios que ya son propietarios de IPhone buscan actualizar sus dispositivos a modelos más recientes como el IPhone 13 Pro-Max que ya está vigente desde Septiembre del 2021. [28] (*Véase la Figura 31) "La disposición del consumidor por países para actualizarse a un dispositivo 5G."*

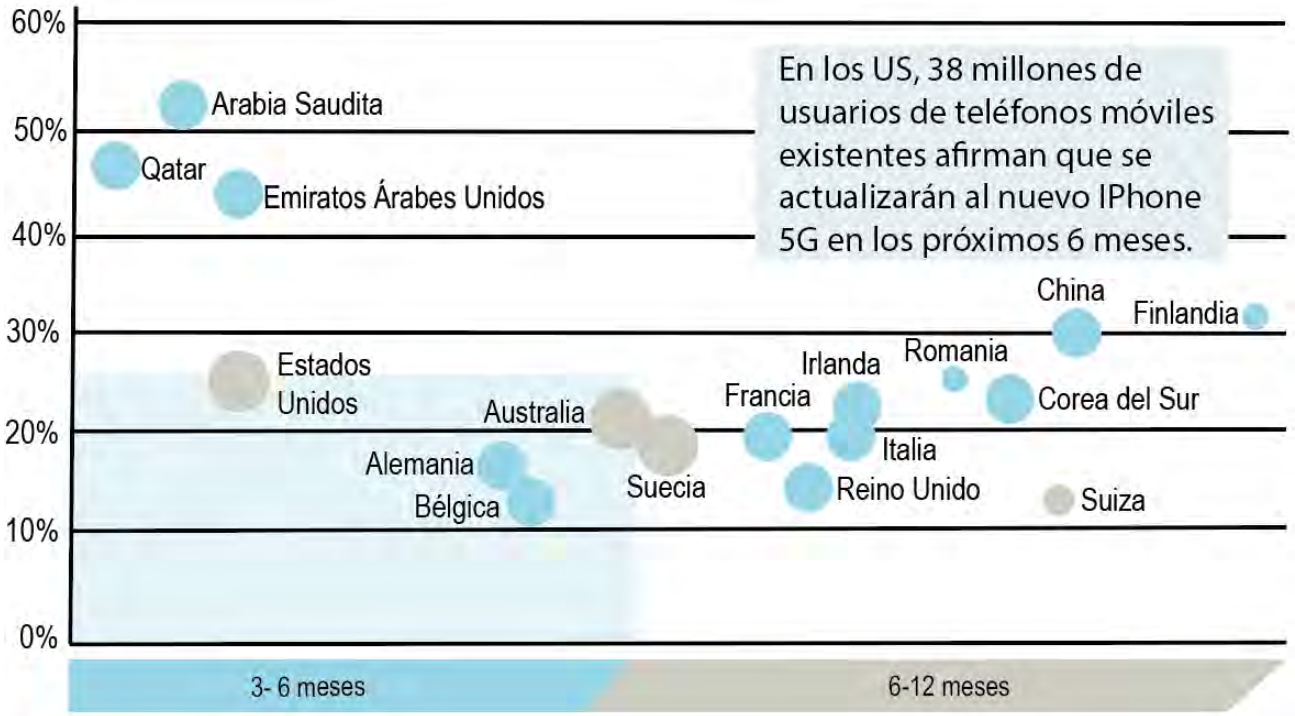


Figura 31 Disposición del consumidor para actualizarse a un dispositivo 5G durante un periodo de 12 meses incluida la transmisión de video. Fuente: Sony Ericcson (2021) [28]

Las medidas de aislamiento que se dio en el 2020 cuando inició la crisis sanitara, ha puesto en evidencia la necesidad de contar con una conectividad confiable, de alta velocidad para solventar las necesidades de la vida diaria de las personas, como puede ser en educación en línea, videoconferencias, Home Office, salud, las compras, etc con el fin de mitigar la propagación del virus. Esas actividades tomaron una forma digital, brindando una plataforma de innovación, nuevas formas de brindar servicios, [27] inclusive surgió un mayor interés en invertir en mercados emergentes servicios digitales mejorados con 5G que ofrecen experiencias de eventos digitales remotos en vivo o en Educación Inmersiva que son libros digitales para niños de Realidad Aumentada. [28]

2.2 Principales componentes 5G

De acuerdo con la definición presentada al inicio del Segundo Capítulo, tenemos que 5G es el conjunto de tecnologías en una sola estructura de Red que ofrece servicios y nuevas funciones mediante Telefonía Móvil. 5G conlleva una variedad de características que veremos más adelante, pero para poder ofrecerlas inclusive para soportar las nuevas aplicaciones, es necesario mencionar los componentes que lo hacen posible, como es la arquitectura de Red, como funciona, que esquemas de modulación complejo utiliza a comparación de otras generaciones, como por ejemplo Mimo Masivo, mmWave y Algoritmos con Módulos de Hardware Avanzado.

Los principales componentes 5G son: (ver Figura 32)

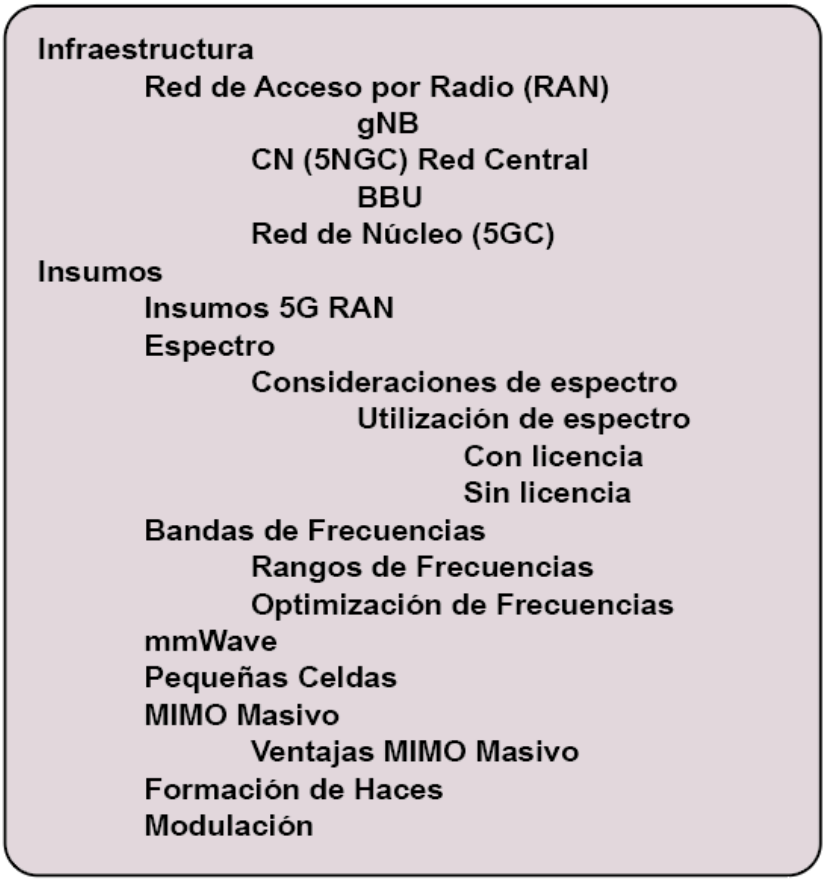


Figura 32 Principales componentes 5G. Fuente: Elaboración propia.

Para lograr la conectividad 5G se necesita la combinación de otras tecnologías, tales como (ver Figura 33): [12]

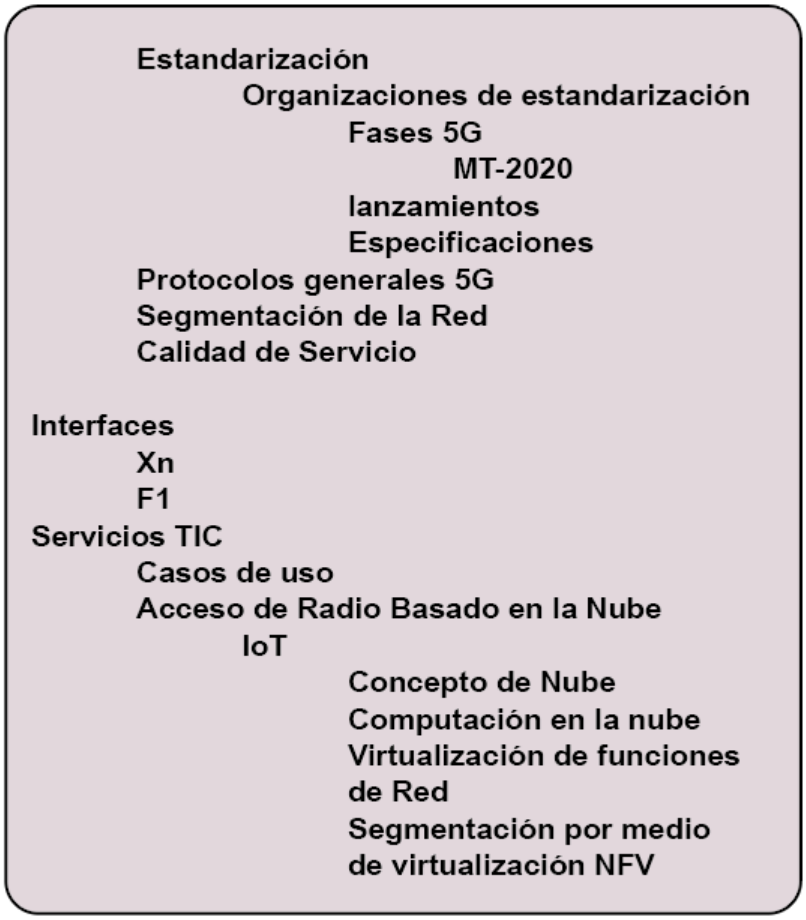


Figura 33 Principales componentes 5G. Fuente: Elaboración propia.

2.2.1 Elementos de la Red 5G

Según plan Colombia (2019) de manera general 5G se compone de insumos, infraestructura, servicios TIC e Interfaz. [22]

2.2.1.1 Infraestructura

Componentes físicos de las redes a través de los cuales se soportan los servicios que permiten 5G, esto incluye Estación Base, fibra óptica, técnicas terrestres y satelitales. [22]

2.2.1.2 Insumos

Dentro de los insumos más importantes para prestar servicios 5G está por ejemplo el espectro radioeléctrico. [22]

2.2.1.3 Interfaz

Aparatos y dispositivos mediante los cuales los usuarios acceden a los diferentes servicios que sobre las tecnologías de la información y las comunicaciones que pueden ofrecer. [22]

2.2.1.4 Servicios TIC

Servicios prestados a través de infraestructura de 5G, donde una parte estará la convergencia de servicios y la otra permitirá la inclusión de servicios como Big Data, comunicaciones M2M, IoT, que requieren alta disponibilidad y baja latencia como vehículos autónomos entre otros. [22]

Según 5G Basics (2021) “5G de Quinta Generación representa una transformación completa de las redes de telecomunicaciones, introduciendo una riqueza de beneficios que allanarán el camino para nuevas capacidades y admitirán la conectividad para aplicaciones como Ciudades Inteligentes, Vehículos Autónomos, Atención Médica y mucho más. [12]

Su funcionamiento se da por medio de la Red de Acceso Radio y Red de Núcleo (ver Figura 34).” [12]

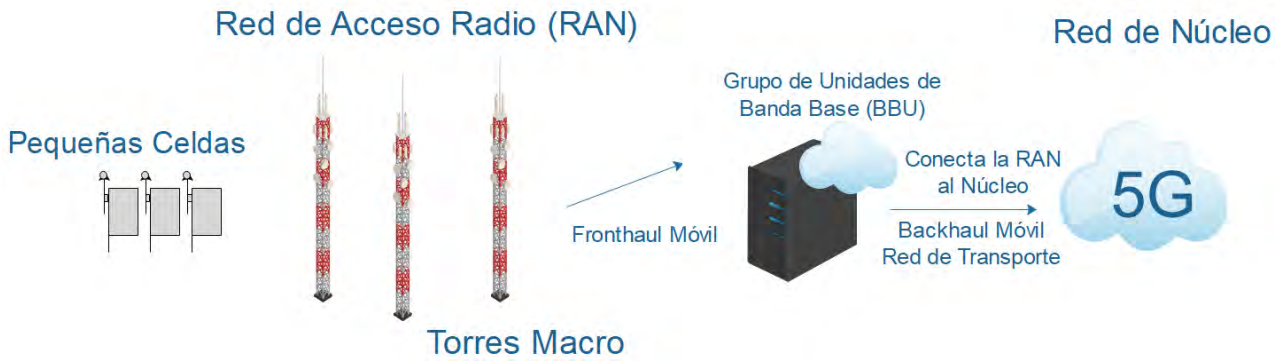


Figura 34 Funcionamiento de la Red 5G. Fuente: CISA (2021) [12]

2.2.1.5 Infraestructura

2.2.1.5.1 Red de Acceso Radio (RAN)

“Es el responsable de definir las funciones, requisitos y que implican el rendimiento de Radio, la capa física y las definiciones de la operación, requisitos de mantenimiento para las pruebas de conformidad para Equipos de Usuario y Estaciones Base.” [30]

“Las Redes 5G aprovecharán al espectro de Banda baja, Media y Alta, lo que requerirá el despliegue de Celdas Pequeñas, además de Macro Torres. Estas pequeñas Celdas servirán como repetidores de señal, proporcionando mayor velocidad, mayor capacidad de Red y mayor confiabilidad en zonas de mayor densidad.” [12] utilizando Fronthaul móvil (fibra óptica) siendo el medio de transporte, para conectar la RAN al núcleo. [12]

Entre las funciones de la RAN tenemos

Supervisar las funciones relacionadas con la radio de la Red en general como la programación, la Gestión de Recursos de Radio, los protocolos de retransmisión, codificación y varios esquemas de múltiples antenas. [30]

Es decir, es la forma que se puede acceder a las frecuencias de Radio y todo lo que implica la comunicación móvil 5G utilizando Macro Torres o Pequeñas Celdas para establecer la conexión.

2.2.1.5.1.1 Insumos 5G RAN

Las tecnologías habilitadoras para 5G RAN, incluyen comunicación mmWave, Múltiples Entradas Múltiples Salidas (MIMO) Masivo, formación de Haces. [20]

2.2.1.5.1.1.1 mmWave

La descripción de mmWave se encuentra en la página 104, 105 y sus Bandas en la 101.

2.2.1.5.1.1.2 Pequeñas Celdas

Las Celdas pequeñas “son nodos de Acceso de Radio de baja potencia controlados por el operador de rango de cobertura de diez o varios centros de metros, incluido los que operan en un espectro con licencia o sin licencia.” [20]

Se utilizan para aumentar la densidad de la Red y mejorar su rendimiento. Con Celdas pequeñas, el tamaño de la Celda se reduce, haciendo un acercamiento más estrecho con el usuario, brindando un mejor servicio a áreas de alto tráfico, como áreas interiores y puntos de acceso. [20] Las Células pequeñas utilizan ondas milimétricas para transmitir y recibir datos, aunque no sean adecuadas en comunicaciones de larga distancia debido a la distorsión de la atmósfera. [20]

5G permite la ubicación cercana de los distintos tipos de células conectadas entre sí. [20] (*Véase la Figura 37), "Arquitectura de Células pequeñas Ultra Tensas" en la página 91.*

2.2.1.5.1.1.3 MIMO Masivo

"Es un tipo de sistema de comunicación, donde la Estación Base (BS) tiene grandes conjuntos de antenas del orden de cientos, que atienden a usuarios, en el orden de decenas en el mismo recurso tiempo-frecuencia. La ventaja de tal sistema es que la BS con múltiples antenas transmite flujos de datos independientes a múltiples usuarios en el mismo recurso de tiempo-frecuencia, logrando velocidades de datos más altas." [32]

A partir de la versión 8 de los estándares establecidos por las SDO [15], V*éase "Evoluciones de las versiones 3GPP" de las páginas 25 – 29.* 3GPP introdujo LTE por primera vez y a su vez el Sistema MIMO 4X4, aunque en las versiones posteriores de los estándares "G" [30] en la versión 10 tiene su evolución a MIMO 8x8 para DL y 4X4 para UL [17] 5G utiliza la evolución de MIMO Masivo con mayor número de antenas de lo habitual. [32] Esto quiere decir que MIMO sólo tiene acceso a decenas de puertos de antenas, [14] mientras 5G cientos de antenas para ampliar la capacidad de comunicaciones. [32]

2.2.1.5.1.1.3.1 Ventajas MIMO Masivo

Algunas ventajas básicas proporcionadas por MIMO Masivo incluyen:

- Ganancia de multiplexación espacial: Enviar flujos de datos independientes a usuarios, ayuda aumentar la velocidad de datos hasta más de diez veces. [32]
- Eficiencia energética: Se reduce la potencia de transmisión del UL y DL. [32]
- Mayor confiabilidad: Disminución de recepción de errores. [32]

- Reducción de costos: El consumo de energía se reduce, permitiendo el despliegue de amplificadores de RF de bajo costo, siendo una inversión de bajo costo. [32]

2.2.1.5.1.1.4 Formación de Haces

Al contar Mimo Masivo con cientos de antenas, se produce “Propagación de Trayectos Múltiples”. *Examine tema en el Capítulo 1, página 23 -24*. Provocando interferencias, por lo cual la Formación de Haces[35] es una solución para que las señales transmitidas sean más eficientes, reduciendo la relación Señal - Ruido. [20] [32]

(Ver la Figura 35) la arquitectura de la Red 5G utilizando MIMO Masivo. [31]

2.2.1.5.2 Nodos

2.2.1.5.2.1 gNB y ng-eNB

La Red de Acceso Por Radio puede tener dos tipos de nodos conectados a la Red Central 5G. [30]

Tabla 28 Nodos conectados a la Red Central. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

Nodos	Descripción
gNB	Sirve a los dispositivos NR que utilizan protocolos del Plano de Usuario y de control NR. [30]
ng-eNB	Para servicios LTE utilizando protocolos de Plano de Control y Usuario LTE. [30]

[35] “Es una técnica que se puede realizar regulando la fase de la señal transmitida desde el canal de cada elemento radiante para obtener el haz principal en dirección particular.” [32] *Para más información verifique libro [32] en la página 13.*

NG-RAN es una Red de Acceso por Radio que incluye ng-eNB par LTE como gNB para NR Acceso por Radio. [30]

Aunque el nombre de los nodos gNB o ng-eNB varíe un poco, las funciones son similares, por ejemplo ambos nodos lógicos son responsables de todas las funciones relacionadas con la Radio en una o varias Células, (para más información sobre Celdas o Células, verifica el inicio del Capítulo 1, página 16 – 18.) como la Gestión de Recursos de Radio (RRM), compartir RAN, establecimiento de conexión, enrutamiento de datos del Plano de Usuario a la UPF e información del Plano de Control a la AMF, así como la Gestión de Sesiones. [18][30]

2.2.1.5.3 Implementación de la Red 5G

La arquitectura de la implementación de la Red 5G se encuentra más adelante.

"Es una implementación estándar de un gNB en el que una Estación Base maneja transmisiones de tres Celdas." [30]

2.2.1.5.4 La Red Central (CN)

"Supervisa las funciones que no están directamente relacionadas con el Acceso por Radio, pero son necesarias para proporcionar una Red completa, permitiendo que muchas tecnologías de Acceso por Radio sean compatibles con la misma Red de Núcleo." [30]

2.2.1.5.4.1 Arquitectura de la Red Central

La arquitectura de la Red Central se encuentra entre las páginas 93 – 96, (ver la Figura 39.) [30]

2.2.1.5.5 Grupo de Unidades de Bandas Base (BBU)

"El BBU Pool Centralizado implementa redes definidas por software y Computación de Borde de Acceso Múltiple para asignar la Red según la necesidad y se conecta unidades remotas ubicadas en Torres Macro a través de Fronthaul Móvil." [12]

2.2.1.5.6 Red de Núcleo

2.2.1.5.6.1 Infraestructura de la Red Central

"Core Network es la columna vertebral de la infraestructura comunicaciones de EE. UU. ruta datos y conecta las diferentes partes de la Red de Acceso." [12]

Mejora LTE conocido como Núcleo de Paquete Evolucionado al agregar tres características nuevas basados en servicios de arquitectura, división del Plano de Control y Plano del Usuario, basándose en los recursos de la Red Central y funcionalidades en vez de nodos. [30]

SDN, NFV y la Computación en la Nube se consideran tecnologías clave para diseñar la parte central de las redes 5G. [20]

2.2.1.5.7 Arquitecturas 5G

2.2.1.5.7.1 Arquitectura genérica 5G basado en servicios y MIMO Masivo

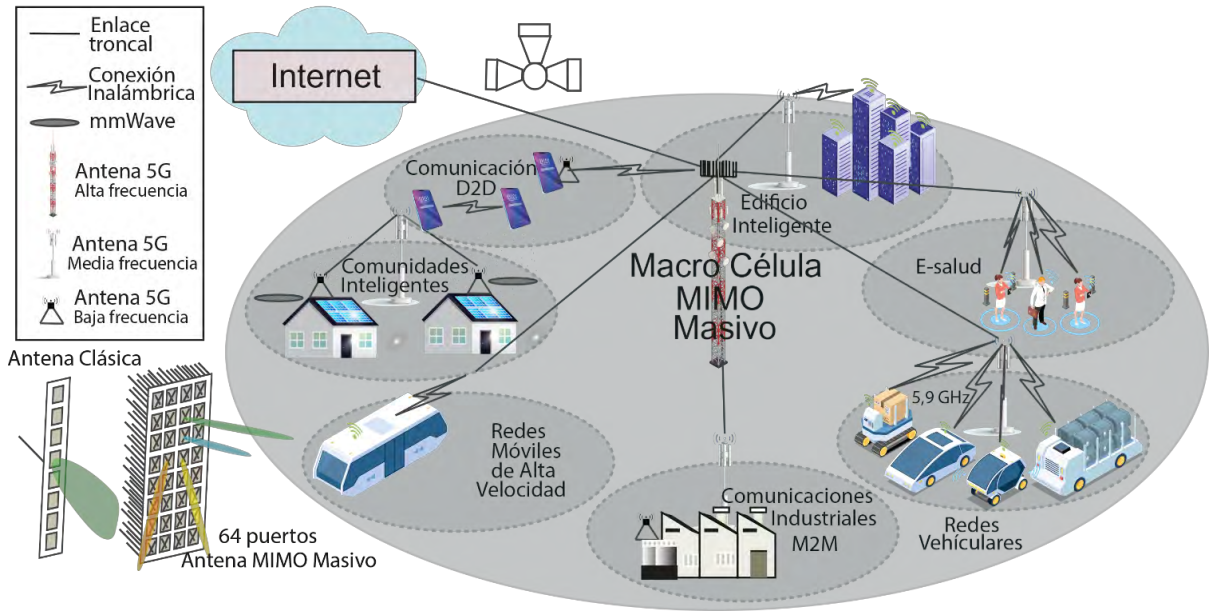


Figura 35 Arquitectura genérica para Sistemas Inalámbricos 5G y MIMO Masivo. Fuente: Elaboración propia basado en [17][20][31]

(Véase la Figura 35), algunos servicios que ofrece 5G y además Mimo Masivo.

La arquitectura de la Red Básica 5G en algunos casos varía mucho según el área de aplicación, la Red 5G debe proporcionar una amplia variedad de servicios en diferentes ubicaciones con velocidades de bits y números de terminales conectados muy variables. [19]

2.2.1.5.7.2 Arquitectura de Formación de Haces

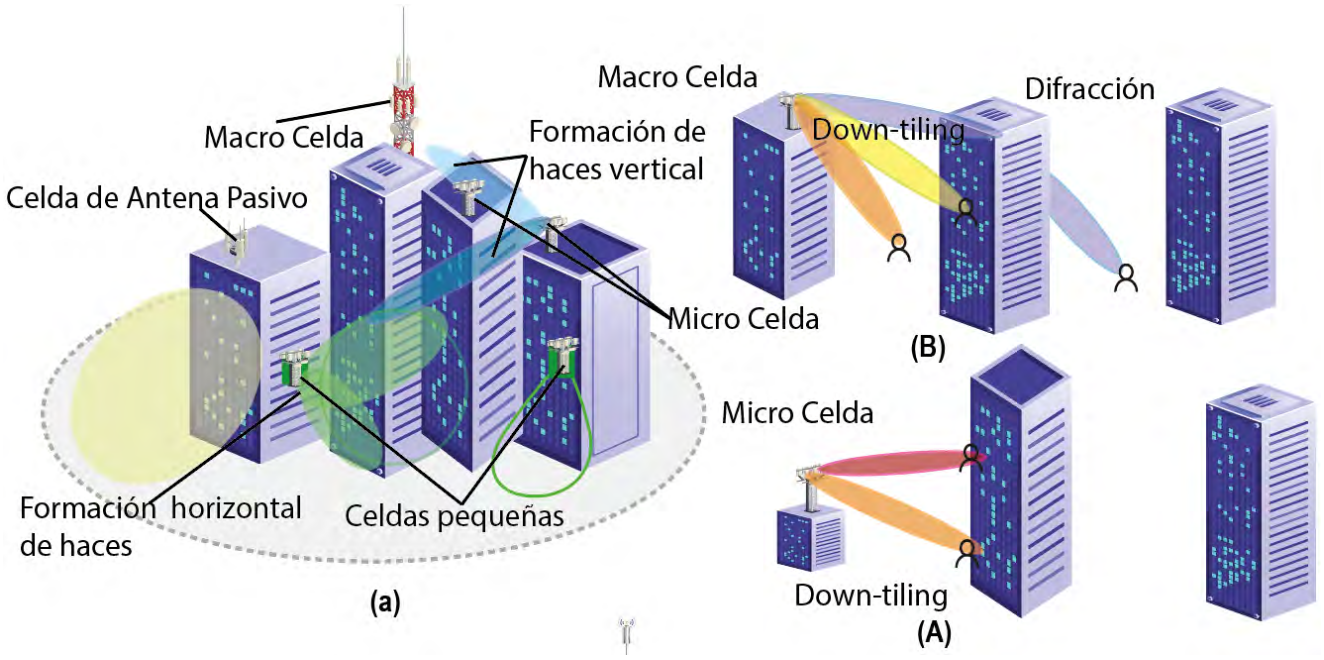


Figura 36 Escenarios de implementación de MIMO de Dimensión Completa (a) sitio de Macrocélulas 3D (colocado sobre el tejado) y (A) Sitio de Macro Celda 3D (colocado debajo del tejado) con Celda pequeña; (b) Formación de Haces para Macrocélulas 3D; y Formación de Haces. Fuente: Abu-Rgheff, Mosa Ali (2020) [17]

(Examine la Figura 36,) la Formación de Haces para la Macrocélula y Microcélula. [17] La señal se envía a usuarios específicos para evitar interferencias, tanto en dirección vertical como horizontal, cubriendo áreas específicas en espacios 3D, permitiendo la difracción de la señal, así como otros trayectos múltiples, siendo una mejora de MIMO Masivo.

“La Formación de Haces específica de la terminal, permite que la BS de MIMO Dimensión completa transmita señales de manera eficaz a las terminales que utiliza, mientras minimiza la interferencia a terminales no deseadas y aumenta considerablemente la eficiencia espectral.” [17]

2.2.1.5.7.3 Arquitectura de Celdas Pequeñas

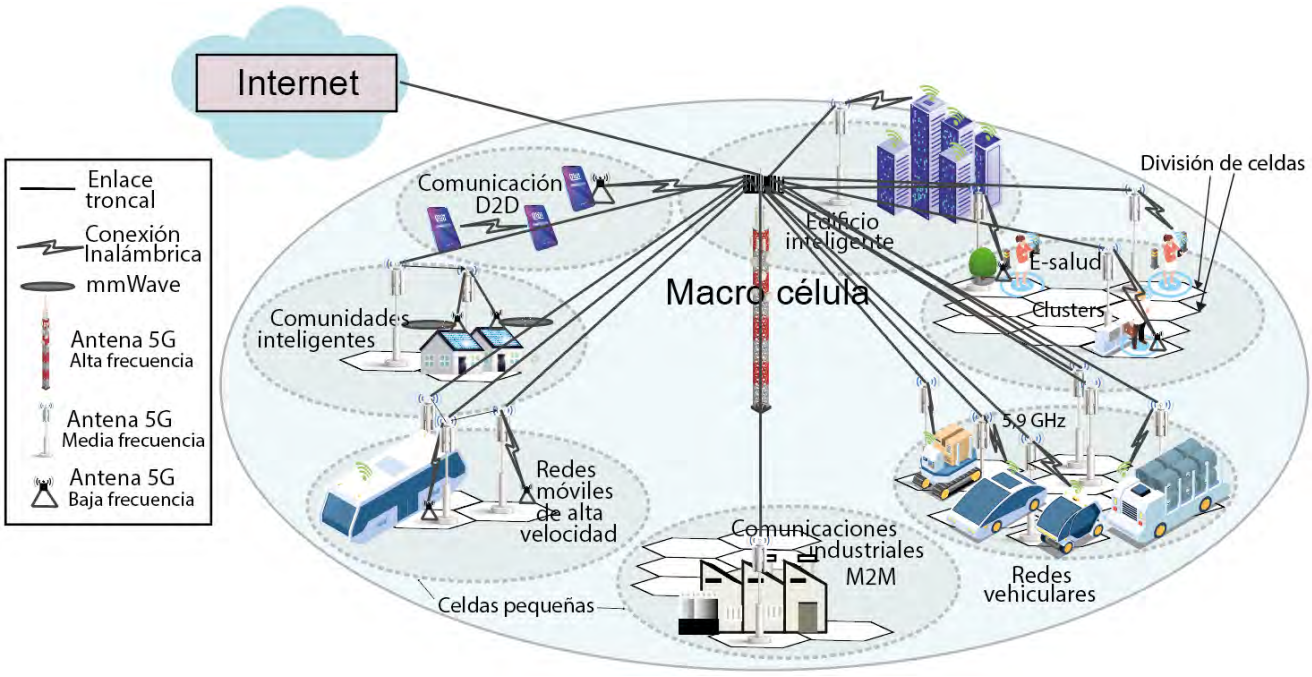


Figura 37 Arquitectura de Células pequeñas Ultra Tensas. Fuente: Elaboración propia basado en [31][20]

Tomando como referencia la Figura 7 en el tema “Organización Celular” página 17, sobre la Figura 37 página 91, la representación de una Macrocélula, basado en 5G, utilizando una estructura en forma hexagonal, dentro de cada hexágono o cada Célula hay una división de Células, con su propia antena o Estación Base. Cada Estación Base radia señal para un número limitado de usuarios. “La Microcélula utiliza una Estación Base de corto alcance dirigido para mejorar la cobertura de los usuarios de interiores o exteriores donde la cobertura macro es insuficiente [14] porque si estamos hablando de una ciudad, existen ciertas zonas donde a pesar de contar con múltiples puertos en las antenas 5G o el número de estas en determinados lugares, por algunos objetos no puede llegar la señal, una Estación Base de corto alcance resuelve estos inconvenientes ya que se puede establecer donde no llega la señal. [14]

2.2.1.5.7.4 Arquitectura de Red de Acceso Radio (RAN) 5G

2.2.1.5.7.4.1 Sitio de tres sectores, implementación de la Red 5G

(Véase la Figura 38,) el gNB está conectado a la Red Central 5G utilizando una Interfaz NG a la UPF a través de la parte de usuario NG, es decir, NG-u y al AMF para compartir carga y redundancia. [30]

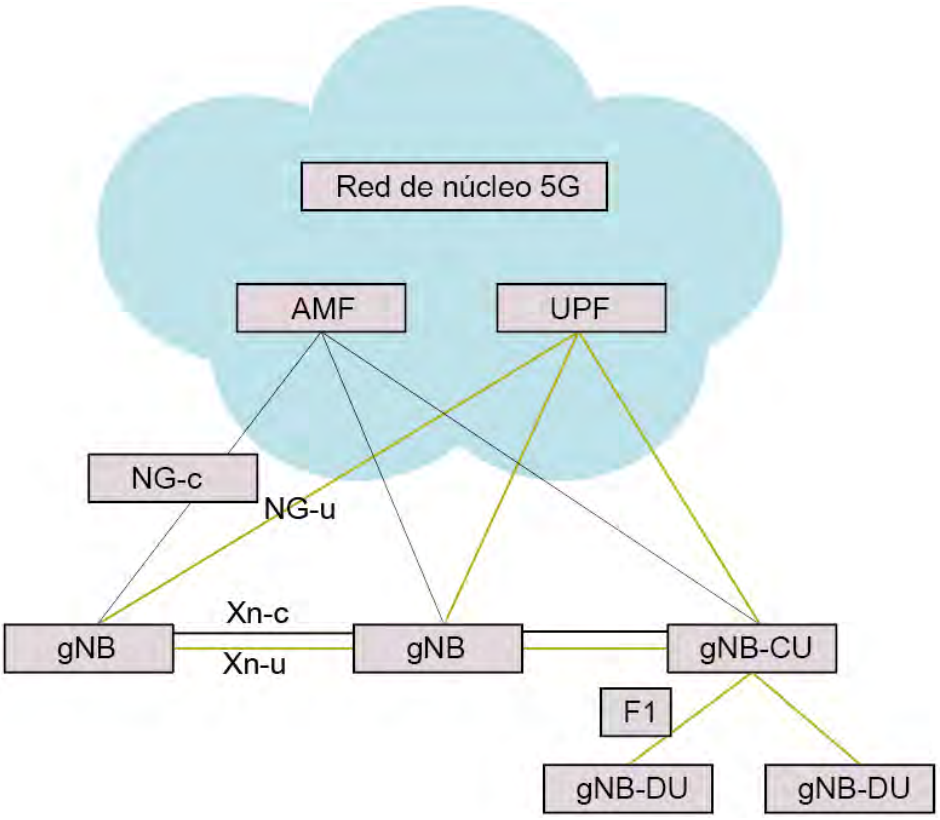


Figura 38 Implementación de la Red 5G.Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

2.2.1.5.7.4.2 Interfaces RAN

La Interfaz Xn que está conectado a la gNB se utiliza principalmente para admitir la movilidad en el modo activo y la conectividad dual sin perdidas entre Celdas vecinas a través de reenvío de paquetes. También para funciones de Gestión de Recursos de Radio Multicelda (RRM). [30]

La Interfaz F1 se utiliza para dividir el gNB en dos componentes:

- La Unidad Central (gNB-CU).
- Y una o dos Unidades Distribuidas (gNB-DU).

Los protocolos RRC, PDCP y SDAP, se encuentran en el gNB-CU, mientras que RLC, MAC y PHY en gNB-DU. [30]

El sistema está conectado inicialmente una sola Celda que maneja transmisiones de UL y DL. Esa Celda tiene el control de todos los flujos de datos, datos de usuario y señalización RRC. [30]

Permitir que el sistema se vincule con la Red a través de varias Celdas puede tener varias ventajas, por ejemplo:

La agregación del Plano de Usuario donde los flujos de datos de varias Celdas se combinan para maximizar la velocidad de los datos. [30]

La separación del Plano de Control y Usuario, donde un nodo maneja el Plano de Control y otro el del usuario. [30]

La conectividad dual entre NR y LTE porque es la base de un servicio no autónomo. [30]

La Celda maestra basada en LTE supervisa la señalización del Plano de Control y la Celda secundaria basada en NR supervisa sólo la señalización del Plano del Usuario. [30]

La conectividad dual entre LTE y NR no formaron parte en la versión 15 de 3GPP, sino más adelante. [30]

“5G RAN proporciona un acceso incomparable a escala masiva para conectar a todos con todo.” [36]

2.2.1.5.7.5 Arquitectura de la Red Central (CN)

La arquitectura de la Red Central 5G basado en servicios.

Enfatiza una división de Plano de Control y de Plano de Usuario con el mismo Ancho de Banda para los dos planos, si se requiere agregar Ancho de Banda adicional en el Plano de Control o viceversa, debería ser sencillo sin afectar el Plano del Usuario. [30]

En la siguiente Figura, se tiene la representación de la arquitectura 5G basado en servicios y sus funcionalidades. [30]

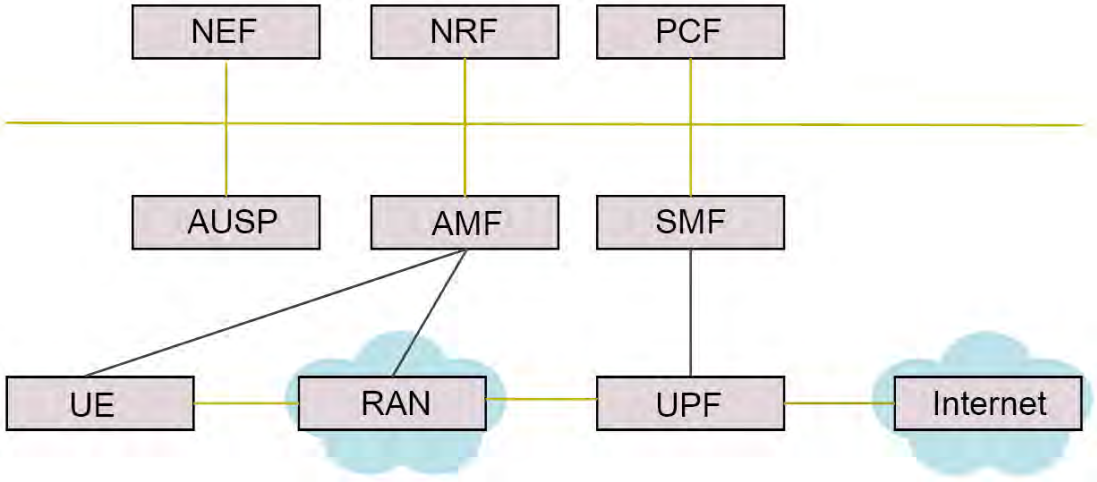


Figura 39 Representación de servicios 5G. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

2.2.1.5.7.6 Funciones básicas de las arquitecturas de Red 5G

Tabla 29 Función del Plano de Usuario. Fuente: Elaboración propia basado en [30]

Nombre	Función
UPF	Se encuentra en la función del Plano de Usuario. [30] "Su función es actuar como un punto de interconexión de sesión de PDU externo a la red de datos." [18]
RAN	Red de Acceso Radio. [30]
Internet	Redes Externas. [30]

En la Tabla 29 podemos ver que entre las funciones de Plano de Usuario tenemos el enrutamiento, reenvío de paquetes, así como la verificación, Gestión de la Calidad de Servicio, (QoS) el filtrado de paquetes y las mediciones de tráfico. [30]

Tabla 30 Función del Plano de Control. Fuente: Elaboración propia basado en [30]

Nombre	Función
UE	Asignación de direcciones IP para el Sistema o Equipo de Usuario. [30]

SMF	Se encuentra dentro de la función de Gestión de Sesiones. [30] El control de cumplimiento de políticas y funciones generales de administración de sesiones. [30]

En la Tabla 30 podemos ver las funciones del Plano de Control, las funciones que se encuentran en el Plano de Usuario también pueden actuar como un punto de anclaje para la movilidad entre NR o RAT. Los componentes que comprenden las funciones del Plano de Control, todas son manejadas por SMF. [30]

Tabla 31 Funciones de Gestión de Acceso y Movilidad. Fuente: Elaboración propia basado en [30]

Nombre	Función
AMF	Función de Gestión de Acceso y Movilidad. [30]
NAS	Estrato sin acceso. Funcionalidad que opera entre la Red Central AMF y el dispositivo. [30]
AS	Estrato de Acceso. [30]

En la Tabla 31 podemos ver los componentes que conforman la Gestión de Acceso y Movilidad, que se encarga de la señalización de control entre la Red Central y el dispositivo, la Seguridad de los datos de usuario, la autenticación y la movilidad del estado inactivo. [30]

Tabla 32 Función de Control de Políticas. Fuente: Elaboración propia basado en [30]

Nombre	Función
PCF	Función de Control de Políticas. [30]
UDM	Gestión de Datos Unificados. [30]
NEF	Función de Exposición de Red. [30]
NRF	Función de Repositorio NR. [30] “Admite la función de descubrimiento de servicios.” [18]

AUSF	Función de Servidor de Autenticación. [30]

Véase la Tabla 32 los componentes de la Función de Control de Políticas, responsables de las credenciales de autenticación y Autorización de Acceso mediante políticas. [30]

Tabla 33 Función de Aplicación. Fuente: Elaboración propia basado en [30]

Nombre	Función
AF	Función de aplicación [30] "Interactúa con la Red Central 3GPP para proporcionar servicios como la influencia de aplicación en el enrutamiento de tráfico o la interacción en el marco de políticas." [15] [18]

2.2.1.5.7.7 Arquitectura Final 5G, según 3GPP

La arquitectura de 5G definido por 3GPP es muy diferente a la arquitectura de generaciones móviles anteriores porque es una mejora importante involucrando la Virtualización de Redes, como una forma de optimizar los recursos de la Red de manera dinámica según la necesidad, a través de Segmentos de Red[36]. Inclusive la Computación en la Nube para procesar y almacenar datos, así como una Nueva Interfaz Aérea de Radio llamado NR "Nuevo Radio 5G", a través de sistemas de modulación más avanzados y soluciones de antenas inteligentes de múltiples arreglos. [18]

NR está basado en servicios, porque admite muchos casos de uso más avanzados, con una capacidad de ofrecer comunicaciones masivas de tipo máquina, una modernización fluida de la Red, y una serie de características únicas. [18]

(Ver la Figura 21,) podemos ver los elementos clave que han estado presentes en las Redes Móviles desde el despliegue y evolución de 2G, 3G y 4G. Junto con 5G, tanto las Redes de Radio como las centrales se renovaran con nuevos elementos e interfaces presentes. [18] Esta es la arquitectura final 5G, según 3GPP.

[36] "El segmento de Red se refiere a una Red lógica que proporciona capacidades y características de Red específicas." [18]

5G se diferencia en la estructura de los servicios y como los brinda. La arquitectura 5G tiene un núcleo más complejo (5GC) llamado “Núcleo 5G”, donde se encuentra dividido en un conjunto de funciones de Red (NF) [18], dado que el encaminamiento de paquetes de extremo a extremo está separado entre el Plano de Control que son los elementos más complejos y de usuario donde se accede a los servicios ya sean datos o Internet, este tiene un camino más corto para poder acceder, por lo tanto, su velocidad es más rápida que generaciones anteriores. [30]

Para más información puede guiarse en la Tabla 17, página 54 el “Resumen de los componentes de las Generaciones Móviles” en la página 49 que se encuentra en el Capítulo 1.

En base a la sección “Definición del Sistema Celular”, página 12 - 13, la Figura 20 “La evolución de la Red Móvil y los elementos de apoyo” en la página 55, que se encuentran en el Capítulo 1, el tema: “Pequeñas Celdas” páginas 85, 86, (ver la Figura 34) “El Funcionamiento de la Red 5G” en el Capítulo 2, y diversos conceptos que se encuentran en la sección “Glosario”, así como los acrónimos:

Se determina que n número de Estaciones Móviles dentro del rango permitido, según la capacidad de usuarios en Pequeñas Celdas, a través de la Interfaz de Radio NR (Aérea[37][14][17]), se comunican con una Estación Base 5G, (gNB)[38] cada gNB a través de sus Unidades de Radio remotas está conectado por medio de Fronthaul,[39] es decir, el Enlace de Fibra Óptica al BBU Pool Centralizado que es el grupo de Unidades de Banda Base, encargado de asignar Red según la necesidad, la BBU en cambio, por medio de Backhaul Móvil, la Red de Transporte conecta la RAN a la Red de Núcleo 5G (5GC) infraestructura de la Red Central encargado de conectar los diferentes partes de la Red de Acceso (RAN). [9][12][18]

Dentro del Núcleo 5G, es decir, NGC se encuentran las funciones del Plano de Control y de Usuario.

En el Plano de Usuario tenemos la UPF, esta interactúa entre la Red 5G y la Red de Datos Externa, “admite la funcionalidad de anclaje de sesión de la PDU, por lo tanto, su función es

[37] “Enlace entre el usuario / dispositivo inalámbrico y la Unidad de Radio Remota.” [14]
[38] “También puede llamarse nodo lógico o Macro Torre.” [18][12]
[39] “Es el enlace entre un grupo de Unidades Banda Base y Unidades de Radio Remotas (RRU).” [18]

actuar como punto de interconexión de sesión PDU externo a la Red.” [18] Y la PDN que es la Interfaz que conecta el Núcleo 5G con la Red.

En el Plano de Control en cambio, el SMF, el AMF, el NF1, NF2, NFn [18][30]

El SMF es una Función de Red que se encarga de la gestión de sesiones. “Establece, modifica y libera sesiones. Gestiona las funciones del cliente y servidor del Protocolo de control Dinámico del Host (DHCP).” [18] “Un Equipo de Usuario Único (UE) puede tener una o más SMF asociadas a la vez, cada una de las cuáles representa una división de la Red.” [15]

AMF encargado de la Gestión de Acceso y Movilidad [30] “admite el cifrado de señales de Estrato Sin Acceso NAS aplicando uno de los nuevos algoritmos de Radio NEA0, 128-NEA1 y 128-NEA2.” [18] “Tiene multitud de funciones incluido el registro, la conexión, accesibilidad, gestión de movilidad, autorización, autenticación de acceso al usuario, entre otros.” [18]

2.2.1.5.7.8 Arquitectura 5g de Roaming y No Roaming

Se encuentra en la Figura 21, *para más información puede consultar el libro “5G Explained” de Jyrki T. J. Pennttinen (2019) de la página 72 al 91.*

2.2.1.5.7.9 Arquitectura de Nube RAN / RAN Virtual

El Tema: “Red de Acceso por Radio Basado en la Nube” en la página 131. Para más información puede consultar el libro “5G Explained” de Jyrki T. J. Pennttinen (2019) de la página 72 al 91.

2.2.1.5.7.10 Arquitectura dividida en RAN

Se encuentra en la Figura 21, para más información puede consultar el libro “5G Explained” de Jyrki T. J. Pennttinen (2019) de la página 72 al 91.

Para lograr la conectividad 5G se necesita la combinación de otras tecnologías, tales como: [12]

2.2.1.6 Insumos

2.2.1.6.1 Espectro 5G

Una de las características principales que hacen única 5G, es la capacidad de manejar recursos a velocidades más rápidas que Generaciones Móviles anteriores, proporcionando la facultad de comunicar simultáneamente gran número de usuarios al mismo tiempo y máquinas.

Para hacerlo posible, 5G implementa Equipos de Radio con soporte extendido de Bandas y Ancho de Banda más avanzados, nuevas Bandas de Frecuencias por debajo o encima de la Banda 6 GHz, que ayudan a las regiones inclusive países a cubrir áreas específicas que requieren frecuencias. [18]

5G necesita el espectro dentro de los 3 rangos de frecuencia clave para brindar cobertura amplia y admitir todos los casos de uso. Los tres rangos son: por debajo de 1 GHz, entre 1-6 GHz y por encima de 6 GHz.

2.2.1.6.1.1 Rangos de Frecuencia del Espectro 5G

2.2.1.6.1.1.1 Bandas Bajas

(Ver la Figura 40) “El espectro por debajo de 1 GHz es para extender la cobertura de Banda Ancha Móvil de alta velocidad a zonas urbanas, suburbanas y rurales y contribuir al soporte de servicios IoT. La expansión de los servicios 5G, más allá de los centros urbanos y dentro de los edificios, no es fácil sin este tipo de espectro radioeléctrico.” [22][33]

“2,5 GHz también es una de las primeras bandas que se están desplegando.” [36]

“Los operadores NAM[40] tienen un Ancho de Banda limitado disponible de 3- 6 GHz, en Europa es considerado el uso de 700 MHz para 5G.” [36] Mientras tanto, en Canadá se ha considerado el espectro por debajo de 3 GHz a 600 MHz, Europa a 1,5 GHz y Latinoamérica a 600 MHz y 700 MHz. [36]

[40] “de Latinoamérica” [36]

Espectro 5G: Bandas bajas para cobertura

Banda 3GPP	Banda de Frecuencia	Modo Dúplex	Región
n71	600 MHz	FDD	NAM
n28	700 MHz	FDD	Europa
n5	850MHz	FDD	NAM
n9	1,7 GHz	FDD	Japón
n3	1,8 GHz	FDD	Europa, Asia
n2, n25	1900 MHz	FDD	NAM
n66, n70	2,1 GHz	FDD	NAM
n41	2,5 GHz	TDD	US, China

5.925 - 7.125 GHz bajo consideracion uso sin licencia en América, con licencia en China
Europa considerando el uso de 700 MHz

Figura 40 Bandas Bajas. Fuente: DropMann Ulrich (2019) [36]

2.2.1.6.1.1.2 Bandas Medias

"El espectro entre 1 y 6 GHz ofrece una buena combinación de cobertura y capacidad para los servicios 5G." El rango 4.5 - 5 GHz y 3.8 - 4.2 GHz para uso Móvil en frecuencias generales (ver Figura 41). [33]

Espectro 5G: Bandas medias

Banda 3GPP	Banda de Frecuencia	Modo Dúplex	Región
n48	CBRS de 3,5 GHz	TDD	
n78	3,3 - 3,8 GHz	TDD	Global
n79	4,4 - 5,0 GHz	TDD	Asia

Nueva consideración de espectro en 3 - 6 GHz
3.7 - 4.2 en discusión en América, Corea y Japón

*CBRS: Servicio de Radio de Banda Ancha para ciudadanos

Figura 41 Bandas Medias. Fuente: DropMann Ulrich (2019) [36]

"Se ha confirmado la Banda 3,5 como principal para las implementaciones iniciales de 5G. Se supone las Bandas 3,7 – 4,2 para convertirse en Bandas importantes, impulsadas por US, Japón y Corea." [36]

2.2.1.6.1.1.2.1 Consideraciones de nuevo espectro entre 3 – 6 GHz

"El espectro en 3.7 – 4.2 GHz se encuentra en consideración en NAM, Corea y Japón." [36]

2.2.1.6.1.1.3 Bandas Altas

"Por encima de 6 GHz para los servicios 5G como Banda Ancha Móvil, para una velocidad ultra-alta. Sin estas velocidades 5G no será capaz de brindar las velocidades de datos más altas." [33] "Las soluciones basadas en Mimo Masivo, la conformación de haces es cada vez más factibles en las frecuencias más elevadas." [21]

2.2.1.6.1.1.3.1 Consideraciones de nuevo espectro por encima de 6 GHz

- "5.925 – 7.125 GHz bajo consideración para uso sin licencia en NAM, uso con licencia en China.
- 5.925 – 6.425 GHz bajo consideración para uso sin licencia en Europa.
- Banda de 40 GHz N259 (39.5 – 43,5 GHz) en estudio en 3GPP." [36]

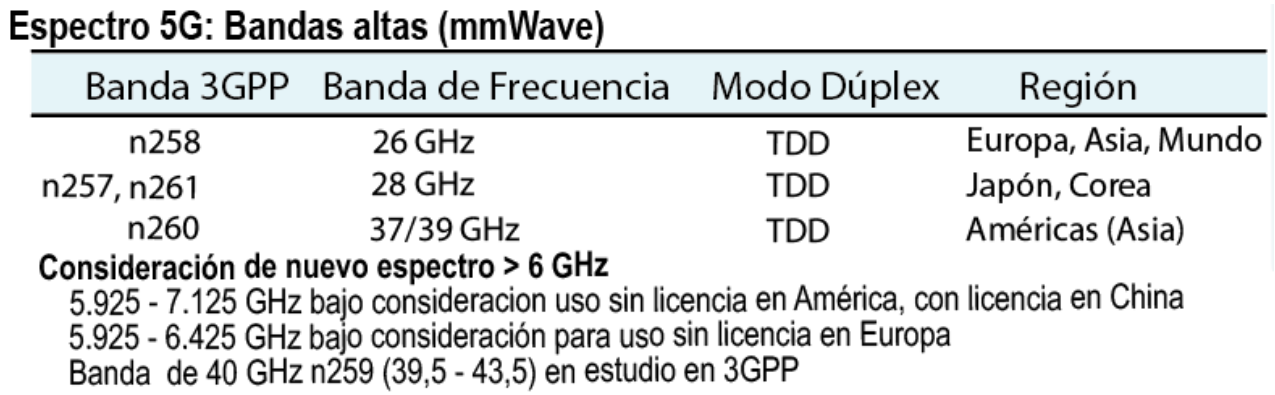


Figura 42 Bandas Altas. Fuente: DropMann Ulrich (2019) [36]

(Examine la Figura 42,) Bandas de alta frecuencia que también se utilizan en mmWave. [32]

2.2.1.6.1.2 Optimización de Frecuencias

Cada día incrementa el número de usuarios en diferentes partes del mundo, por lo que existe una demanda inminente que oferta para las frecuencias, por lo tanto, el Enfoque de Espacio en Blanco[41] es un método eficaz para optimizar la utilización de frecuencias. Además

[41] "Bandas compartidas que pueden ser utilizadas por diferentes partes interesadas." [18]

de los métodos tradicionales comprando derechos para la utilización de frecuencias con licencia. [18]

“Por lo tanto, las áreas de cobertura más grandes por Celda de Radio, las frecuencias deben ser bajas, mientras que las áreas de cobertura con mayor capacidad dependen de las frecuencias más altas.” [18] Esto quiere decir, que “las frecuencias más altas proporcionan la capacidad muy necesaria para las ubicaciones limitadas y las frecuencias muy bajas garantizan el funcionamiento básico de servicios 5G en las áreas más amplias.” [18]

2.2.1.6.1.2.1 Utilización del espectro

La utilización del espectro puede llevarse a cabo de dos formas:

2.2.1.6.1.2.1.1 Con licencia

Véase glosario para tal definición.[15]

“A los operadores móviles se le asignan licencias para obtener algunos derechos sobre una parte del espectro y así poner en funcionamiento los servicios que le proporciona a los usuarios, como voz y datos.” [21]

“El espectro con licencia es esencial para garantizar las grandes inversiones en la red a largo plazo necesarias para 5G y poder prestar servicios de alta calidad.” [33]

2.2.1.6.1.2.1.2 Sin licencia

El espectro sin licencia es complementario a la utilización del espectro con licencia, ya que al combinar ambos espectros aumenta el uso del espectro sin licencia y minimiza el riesgo de una mala experiencia de usuarios si las bandas están saturadas. [33]

2.2.1.6.1.3 Bandas de Frecuencia 5G

Las Bandas 5G están definidas por 3GPP. *Véase en el Capítulo 1 para más información de 3GPP.* Y se establecen en el TS 38.104. [18]

Banda de Frecuencia NR	UL (Up Link)	DL (Enlace Descentente)	Modo Dúplex	Región
n1	1920 MHz - 1980 MHz	2110 MHz - 2170 MHz	FDD	Europa, Asia
n2	1850 MHz - 1910 MHz	1930 MHz - 1990 MHz	FDD	Américas (Asía)
n3	1710 MHz - 1785 MHz	1805 MHz - 1880 MHz	FDD	Europa, Asia (Américas)
n5	824 MHz - 849 MHz	869 MHz - 894 MHz	FDD	Américas (Asía)
n7	2500 MHz - 2570 MHz	2620 MHz - 2690 MHz	FDD	Europa, Asía
n8	880 MHz - 9150 MHz	925 MHz - 960 MHz	FDD	Europa, Asia
n12	699 MHz - 716 MHz	729 MHz - 746 MHz	FDD	
n20	832 MHz - 862 MHz	791 MHz - 821 MHz	FDD	
n25	1850 MHz - 1915 MHz	1930 MHz - 1995 MHz	FDD	
n28	703 MHz - 748 MHz	758 MHz - 803 MHz	FDD	
n34	2010 MHz - 2025 MHz	2010 MHz - 2025 MHz	TDD	
n38	2570 MHz - 2620 MHz	2570 MHz - 2620 MHz	TDD	Europa
n39	1880 MHz - 1920 MHz	1880 MHz - 1920 MHz	TDD	
n40	2300 MHz - 2400 MHz	2300 MHz - 2400 MHz	TDD	
n41	2496 MHz - 2690 MHz	2496 MHz - 2690 MHz	TDD	US, China
n50	1432 MHz - 1517 MHz	1432 MHz - 1517 MHz	TDD	
n51	1427 MHz - 1432 MHz	1427 MHz - 1432 MHz	TDD	
n66	1710 MHz - 1780 MHz	2110 MHz - 2200 MHz	FDD	Américas
n70	1695 MHz - 1710 MHz	1995 MHz - 2020 MHz	FDD	
n71	663 MHz - 698 MHz	617 MHz - 652 MHz	FDD	Américas
n74	1427 MHz - 1470 MHz	1475 MHz - 1518 MHz	FDD	Japón
n75	-	1432 MHz - 1517 MHz	SDL	Europa
n76	-	1427 MHz - 1432 MHz	SDL	Europa
n77	3300 MHz - 4200 MHz	3300 MHz - 4200 MHz	TDD	Europa, Asia
n78	3300 MHz - 3800 MHz	3300 MHz - 3800 MHz	TDD	Europa, Asia
n79	4400 MHz - 5000 MHz	4400 MHz - 5000 MHz	TDD	Asia
n80	1710 MHz - 1785 MHz	-	SUL	
n81	880 MHz - 915 MHz	-	SUL	
n82	832 MHz - 862 MHz	-	SUL	
n83	703 MHz - 748 MHz	-	SUL	
n84	1920 MHz - 1980 MHz	-	SUL	
n86	1710 MHz - 1780 MHz	-	SUL	
n257	26 500.0 MHz - 29 500, 0 MHz	26 500,0 MHz - 29 500, 0 MHz	TDD	Europa, Asía, Mundo
n258	24 250, 0 MHz - 27 500, 0 MHz	24 250,0 MHz - 27 500, 0 MHz	TDD	Japón, Corea
n260	37 000, 0 MHz - 40 000, 0 MHz	37 000,0 MHz - 40000, 0 MHz	TDD	

Figura 43 Bandas de Frecuencias según 3GPP para 5G. Fuente: Elaboración propia basado en [15][18][19]

(Ver la Figura 43), este refiere las Bandas de Frecuencias 5G, según 3GPP para la transmisión de Radio 5G NR (Nuevo Radio), para la dirección de Enlace Ascendente (UL) o Enlace Descendente (DL). También indica que método de separación direccional utilizará, si FDD[42] o

[42] Duplexación por División de Frecuencia. [19]

TDD[43] según el canal NR utilizado. SUL[44] o SDL[45] para permitir una tasa de bits más alta de manera asimétrica, en comparación de FDD y TDD. [19]

Las Bandas de Frecuencia que utiliza 5G, de la n1-n16 comparte las mismas bandas con LTE, de la misma manera del 1-76 con las Bandas de 4G LTE, en cambio, 5G NR tiene nuevas Bandas a utilizar, [18] debido a la limitación en el número de Bandas FDD disponibles, [36] estas son: n77-n84, n257, n258, n260. [18] [32]

“Las Bandas de Frecuencia son asignados por una autoridad reguladora para una región geográfica específica exclusivamente para un operador de Red, por ejemplo en una subasta.” [19]

“El espectro es una fuente de ingresos por parte del gobierno.” [14] Cobrar por el espectro también proporciona dinero para el Estado.” [22] “Una subasta bien diseñada adjudica el espectro como valor a quienes lo soliciten dándole un uso eficiente.” [22]

La asignación de espectro es necesaria no sólo en la Interfaz Aérea, sino también en el Backhaul y hasta el Fronthaul. En la Interfaz Aérea se requiriere la mayor parte del espectro. [14]

2.2.1.6.2 mmWave

Existen distintos desafíos críticos como las Bandas con Licencia saturadas, debido al número creciente de dispositivos y la utilización de servicios que exigen una alta velocidad de datos, inclusive el costo por la utilización de las bandas con licencia para los proveedores de servicios. [32] Al ser muy caros le dan un mejor uso. [22]

La utilización eficiente del espectro de Radio, la reconstrucción de técnicas de comunicación de la capa física [32] hace posible que se puedan tener velocidades 5G hasta decenas de Gbps a velocidad máxima de datos. [20] Estos técnicas son:

- El despliegue de Células pequeñas. *Véase tema: “Pequeñas Celdas” en la página 85 - 86, en el Capítulo 2.*

[43] Duplexación por División de Tiempo. [19]
[44] Enlace Ascendente Suplementario. [19]
[45] Enlace Descendiente Suplementario. [19]

- La utilización de Bandas de Frecuencia de ondas milimétricas (mmWave) infrautilizadas. [32]

mmWave es una Red Celular que utiliza señales de alta frecuencia, [32] "se adapta a las redes 5G densas de Células pequeñas en Puntos de Acceso urbanos, donde la capacidad adicional es crucial." [33] "Utiliza frecuencias en el rango de 30 a 300 GHz, con las longitudes correspondientes entre 10 mm y 1 mm." [20] "28 GHz es la Banda principal para el despliegue de mmWave, seguido por 37 / 39 GHz." [36]

Si hacemos una comparativa entre las Generaciones Anteriores Móviles y 5G: *véase tema: "Evolución de la Telefonía" que se encuentra en el Capítulo 1, página 32 – 48, específicamente la página 49.* Podemos ver que las Bandas de Frecuencias que utilizan las generaciones anteriores se encuentran entre el rango 700 MHz a 3 GHz [20], es decir, Bandas Sub-6 GHz. [33] Este rango de frecuencias no es suficiente para 5G, se necesita expandir el rango de Ancho de Banda explorando Bandas de Frecuencia altas que no han sido ocupadas y éstas son las que se encuentran por encima de 10 GHz. [20] [32] "El uso de frecuencias más amplias, admiten velocidades y cantidades de tráfico más altas." [37]

mmWave trae muchos beneficios para 5G por ejemplo un rango más extenso de Ancho de Banda que ayuda a mejorar la velocidad de datos. [20]

2.2.1.6.3 Modulación

La modulación LTE se encuentra desde la página 46. Utiliza sistemas de comunicación QPSK, 16QAM y 64QAM, mientras que 5G utiliza 254QAM, (véase Figura 16,) [18] y para la codificación turbo o convolucional. La creación de la señal OFDM se basa en IFFT que es la versión practica de la transformada de Fourier (DFT) y relativamente fácil de implementar ya que existen componentes estándar para el cálculo de la transformación. [18]

Véase página 40 - 47 del Capítulo 1 en tema: "LTE" para mayor comprensión.

2.2.1.6.4 Estandarización 5G

"El desarrollo de políticas y estándares sirve como base para asegurar los 5G una infraestructura futura de comunicaciones." [43]

2.2.1.6.4.1 Organizaciones de estandarización

"Algunos organismos de estandarización clave que influyen en 5G, ya sea directa o indirectamente, así como los que se ocupan de la estandarización de IoT," [18] son: 3GPP, UIT, IEEE, GSMA, NIST, OneM2M, CSA, NGMN, NHTSA, ISO/IEC, OWASP, OMA, 5GAA e IETF. [18]

2.2.1.6.4.1.1 3GPP (SDO)

3GPP *se describe en las páginas 25 – 29, del Capítulo 1.*

"3GPP se toma como base para las implementaciones de Sistemas y Redes 5G, porque es la más completa y detallada, sobre todas los Organismos de Estandarización." [19]

"3GPP define la tecnología de Radio 5G bajo el nombre NR, mientras que la Red Central (CN) se conoce como NGC (Núcleo de Próxima Generación)." [18]

Se ha ampliado para cubrir la Red de Área Amplia de Baja Potencia (LPWAN), incluyendo M2M de baja tasa de bits, aspectos de Seguridad 5G, Algoritmos 5G, derivación de claves, Seguridad en el Backhaul y SIM. [18]

2.2.1.6.4.1.1.1 Fases 5G

"3GPP funciona utilizando una metodología de 3 etapas o fases" [35] "que derivan las versiones o lanzamientos de la estandarización 3GPP." [20]

2.2.1.6.4.1.1.1.1 Fase Pre-5G

Comenzó a principios del 2015, es la fase de estudio, por ejemplo, sobre *Habilitadores de Tecnología de Nuevos Servicios y Mercados* (SMARTER) con el objetivo de desarrollar casos de uso de alto nivel, por ejemplo; eMBB[46], mIoT[47] y NeO[48]. [20]

[46] "Ancho de Banda Móvil Mejorado." [20]

[47] "Internet de las Cosas Masivo." [20]

[48] "Operación de Red." [20]

Desde la perspectiva RAN, sobre el Modelo de Canal para las frecuencias del espectro por encima de 6 GHz, así como los requisitos y alcance del Nuevo Acceso Radio 5G. [20]

2.2.1.6.4.1.1.1.2 5G Fase I

Después de finalizar la Fase Pre-5G, se inicia la primera fase de estandarización de soluciones relacionadas con 5G, en donde se proponen elementos de trabajo para su aprobación. [20]

“La Fase I se centra en casos de uso para mejorar la Banda Ancha Móvil, así como Baja Latencia y Alta Confiabilidad. NR Nuevo Radio se estandariza en esta fase, donde el rango de Frecuencias está por debajo de 6 GHz,” [20] es decir, en esta fase se basa en “los servicios que proporcionará el sistema destino desde la perspectiva del usuario.” [19]

2.2.1.6.4.1.1.1.3 5G Fase II

La Fase II de 5G optimiza la Banda Ancha Móvil mejorada y todos los casos de uso 5G. La estandarización de NR con nuevas características como el uso de la frecuencia más alta usando mmWave y aspectos de Seguridad, [20] es decir, “las funciones de la Red necesarias y su interacción se resuelven de acuerdo con los requisitos de servicio.” [19]

2.2.1.6.4.1.1.1.4 5G Fase III

“Especifica las funciones de conmutación concretas y protocolos requeridos para los servicios de la Etapa I.” [19]

2.2.1.6.4.1.1.2 Lanzamientos 3GPP

De acuerdo con el enfoque de fases, tenemos:

2.2.1.6.4.1.1.2.1 Versión 15

“La versión 15 (Fase I 5G) se estandarizó para el Primer Sistema 5G completo a mediados del 2019,” [19] con la versión de 5G /New Radio[49] (NR) [30] y un conjunto de nuevas funciones como parte de la evolución LTE. [30] LTE sigue evolucionando de manera paralela juntamente con NR y es muy importante en el Acceso de Radio 5G. [15] “El modo no autónomo (NSA) de NR fue aprobado por 3GPP en diciembre del 2017. El modo autónomo (SA) se completó en diciembre del 2018 implicando la separación de los Planos de Control y de Usuario en la nueva arquitectura 5G.” [18]

2.2.1.6.4.1.1.2.2 Versión 16

(Fase II 5G) “Con una fecha objetivo de finales del 2020, debido a la pandemia COVID-19, está en marcha, con un Sistema objetivo IMT-2020 definido por la UIT,” [19] “incluye mejoras y extensiones de NR como parte del primer paso en la evolución de NR, junto con extensiones y mejoras adicionales a LTE.” [30][35]

2.2.1.6.4.1.1.2.3 Versión 17

“Principal actividad del 3GPP durante el 2020 y 2021.” [30] “El trabajo en la versión 17 ha comenzado, se espera que se complete en primavera del 2022, por la pandemia.” [19]

(Véase la Figura 44,) los lanzamientos de las versiones del 15 al 17 del 3GPP.

[49] “Nueva Interfaz de Radio NR de 3GPP. Es el nuevo acceso por Radio 5G. Tanto LTE como NR han sido desarrollados por 3GPP.” [15]

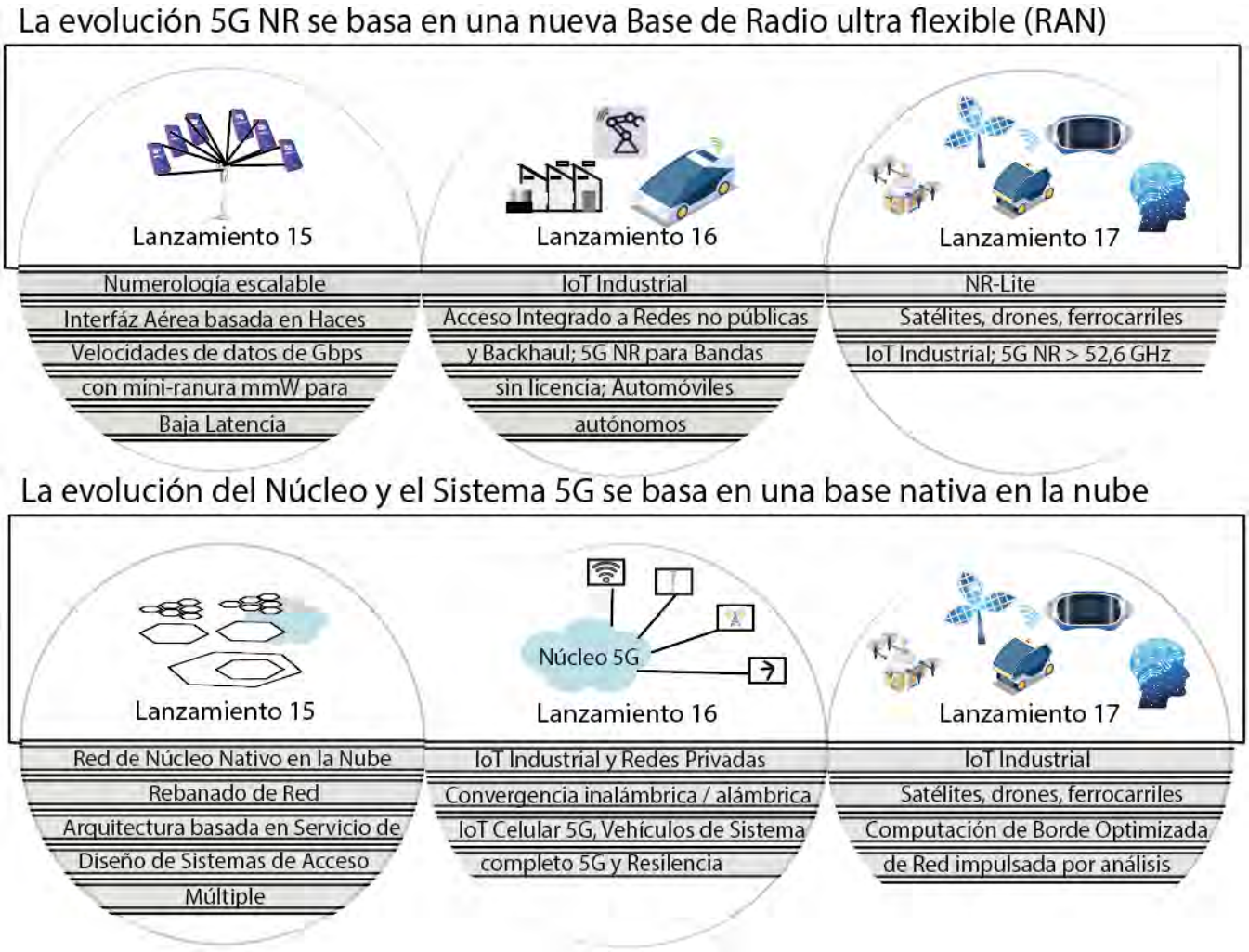


Figura 44 Evolución de RN y Núcleo 5G basado en 3GPP. Fuente: Dropmann Ulrich (2019) [36]

2.2.1.6.4.1.1.3 Especificaciones 3GPP

Las principales especificaciones 3GPP son:

3GPP TS 38.214 Procedimiento de Capa Física NR

Red de Acceso por Radio del grupo de especificaciones técnicas (Etapa I)

- NR
- Procedimientos de Capa Física para Datos.

3GPP TS 38.300 Arquitectura del Protocolo NR

Red de Acceso por Radio del grupo de especificaciones técnicas (Etapa II)

- NR
- NR y NG-RAN descripción general

2.2.1.6.4.1.1.3.1 NR

"5G NR es una Nueva Interfaz Aérea, es decir, la parte del circuito entre el dispositivo Móvil (UE) y la BS activa." [18]

Esta especificación define las siguientes funcionalidades NR

- Arquitectura de Protocolo y División Funcional.
- Interfaces.
- Arquitectura de Protocolo de Radio.
- Movilidad.
- Calidad de Servicio (QoS).
- Seguridad.
- Capas de Control de Acceso al Medio.

3GPP TS 23.501 v15.5.0 Arquitectura 5G CN

Servicios del grupo de especificaciones técnicas y aspectos del sistema (Etapa II).

3GPP TS 29.501v15.3.0 Basado en servicios 5G CN

Terminales y Red Principal del grupo de especificaciones técnicas (Etapa III).

- Arquitectura del sistema 5G. [18]
- Funciones y procedimientos de Red 5G. [18]

[36]

2.2.1.6.4.1.2 Unión Internacional de Telecomunicaciones

Véase páginas 30, 31 en el Capítulo 1.

2.2.1.6.4.1.2.1 UIT-R

2.2.1.6.4.1.2.1.1 Especificación UIT-R

UIT-R SG5 (Comisión de Estudio 5 [19] o Grupo de Trabajo 5D [15]) WP5D (Working Party 5D: IMT-Systems) para aspectos generales del Sistema Radio. [19] Incluidas las cuestiones técnicas, operacionales y relacionadas con el espectro. [15]

WP5D “Es responsable de los aspectos generales del sistema radioeléctrico de los Sistemas de Telecomunicaciones Móviles Internacionales (IMT) a nivel general.” [38]

2.2.1.6.4.1.2.2 UIT-T

2.2.1.6.4.1.2.2.1 Especificación UIT-T

UIT-T SG13 (Redes Futuras con el enfoque de IMT-2020, Computación en la Nube e infraestructuras de Red Confiables) para los aspectos de Red. [19]

La UIT establece expectativas de rendimiento para 5G y lo registra en la IMT - 2020. [18]

2.2.1.6.4.1.3 IEEE

“El Instituto de Ingenieros Eléctricos Electrónicos (IEEE) incluye aspectos para la conectividad IoT.” [18] La serie IEEE St. 1363 para la criptografía de clave pública, variantes como IEEE 802.11p diseñados para comunicaciones vehículo a vehículo.

2.2.1.6.4.1.4 GSMA

“Participa en la estandarización de Gestión de Suscripciones y el Módulo de Identidad del Suscriptor Integrado (eSIM) y su desarrollo para M2M y el entorno del consumidor.” [18]

2.2.1.6.4.1.5 NIST

El Instituto de Tecnología de Estándares (NIST) de EE. UU. “Desarrolla marcos de ciberseguridad para abordar la infraestructura crítica, incluida el espacio IoT / M2M.” [18] Centrándose en la Seguridad y privacidad de los usuarios. [18]

2.2.1.6.4.1.6 OneM2M

“La arquitectura y estándares de OneM2M para las comunicaciones M2M están diseñadas para ser aplicadas en muchas industrias diferentes.” [18] “Trabaja en e-Salud y Telemedicina, Automatización Industrial y Doméstica.” [18]

2.2.1.6.4.1.7 CSA

“La Alianza de Seguridad en la Nube (CSA) es una organización sin fines de lucro que promueve el uso de prácticas para brindar garantía de Seguridad dentro de la computación en la nube.” [18]

2.2.1.6.4.1.8 NGMN

“Las Redes Móviles de Próxima Generación (NGMN) son relevantes para las tecnologías de Red, así como IoT.” [18] “NGMN ha lanzado los proyectos: “Eficiencias de implementación y espectro”, “Convergencia RAN” y “Comunicaciones de largo alcance extremas para una cobertura rural profunda.” [18]

2.2.1.6.4.1.9 NHTSA

“La Administración Nacional de Seguridad y Transporte de Carreteras (NHTSA) mejora la Seguridad y movilidad en las carreteras de EE. UU. También investiga la tecnología de vehículos conectados y las comunicaciones de información de Seguridad y movilidad entre sí.” [18]

2.2.1.6.4.1.10 ETSI (SDO)

“Ejecuta la estandarización de Seguridad en UICC y su evolución bajo el término SSP[50].” [18] “El Comité Técnico (TC) M2M de ETSI es un grupo relevante para el desarrollo de IoT en ETSI,” [18] y estándares de virtualización. [35]

2.2.1.6.4.1.11 ISO/IEC

“La Organización Internacional de Normalización (ISO) / Comisión Electrotécnica Internacional (IEC) es un organismo elemental para la estandarización de la tecnología de tarjetas inteligentes.” [18] También está relacionado con la Seguridad de IoT. [18]

2.2.1.6.4.1.12 OWASP

“El Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP) se centra en mejorar la Seguridad del Software.” [18] También “proporciona información de Áreas de Superficie de Ataque de IoT, guías de prueba y mantiene una lista de las 10 principales vulnerabilidades de IoT.” [18]

2.2.1.6.4.1.13 OMA

“Open Mobile Alliance (OMA) ha desarrollado la Gestión de Dispositivos DM. OMA LightweightM2M tiene como objetivo optimizar las comunicaciones seguras entre todos los dispositivos, especialmente los económicos.” [18]

2.2.1.6.4.1.14 5GAA

“La misión de la Asociación Automotriz 5G (5GAA) es desarrollar, probar y promover soluciones de comunicaciones, iniciar su estandarización y acelerar la disponibilidad comercial, así como las necesidades de Seguridad vial con aplicaciones como la conducción autónoma, acceso ubicuo a servicios e integración de Ciudades y Transportes Inteligentes.” [18]

[50] “Plataforma Segura Inteligente.” [18]

2.2.1.6.4.1.15 IETF

"Desarrolla el protocolo CoAP[51] y la adaptación a la Seguridad de comunicación actual para su uso con CoAP." [18]

2.2.1.6.5 IMT-2020

> Como se dijo anteriormente, "China formó el grupo de promoción IMT-2020 para promover la infraestructura y el desarrollo de 5G dirigiendo las pruebas del país y otras actividades." [14]

IMT-2020 "es un programa para describir 5G, como un paso de la próxima evolución, después del IMT-2000 e IMT-Advanced, también prepara el escenario para las actividades internacionales de investigación de 5G[52]." [18]

"La especificación UIT-R M.2083 describe los escenarios de uso esperados y sus capacidades requeridas de las IMT-2020." [15]

2.2.1.6.6 Protocolos Generales 5G

Los protocolos 5G se distribuyen en la Capa 1, 2 y 3. [18]

Tabla 34 Capas 5G que especifican los protocolos. Fuente: Jyrki T. J. Pennttinen (2019) [18]

Capa	Descripción	Funciones
Capa 1	Física	Capa Física.
Capa 2	Enlace de Datos	Incluye MAC, Control de Enlace de Radio (RLC) y Protocolo de Convergencia de Datos en Paquetes.
Capa 3	Red	Capa de Control de Recursos de Radio (RRC).

[51] "Protocolo de Aplicación Restringida." [18]

[52] Los estándares 3GPP, UIT, etc. se establecen en las IMT según la Generación Móvil.

2.2.1.6.6.1 Capa 1

"Incluye las siguientes funcionalidades:

- Detección de errores en los canales de transporte, codificación de errores de reenvío (FEC) y decodificación.
- Transporte codificado, mapeo de tasas de canales físicos.
- Sincronización en dominios de frecuencia y tiempo.
- Mediciones de Radio e informes de características de Radio.
- Procesamiento de Antenas de Entrada y Salida Múltiples (MIMO), formación de Haces y Gestión de Diversidad de Transmisión."

[18]

2.2.1.6.6.2 Capa 2

"Se refiere a funcionalidades 5G MAC, RLC y PDCP. Para MAC incluyen:

- Gestión de Haz de Antena.
- Mapeo de canales lógicos y de transporte.
- Concatenación de la Unidad de Datos de Servicio MAC (SDU) del canal lógico al bloque de transporte (TB).

Para las RLC, las funciones de la Capa 2 incluyen:

Transferencia PDU de la Capa superior (Red).

- Restablecimiento de 5G-RLC.
- Corrección de errores basada en ARQ de transferencia de datos AM, detención de errores de Protocolo y Segmentación.
- Reordenamiento de PD 5G RLC de transferencia de datos en mono no conocido (UM) y modo de reconocimiento (AM), detención de paquetes duplicados y segmentación.

Para el PDPC, las funciones de la Capa 2 incluyen:

- Transferencia de datos de usuario.
- Entrega en secuencia de PDU de capa superior y detección de duplicados de SDU de capa inferior.
- Cifrado y descifrado basado en el estándar de cifrado avanzado obligatorio (AES).
- Cifrado del Plano de Usuario y de la integridad.
- Transferencia de datos en el Plano de Control.” [18]

2.2.1.6.6.3 Capa 3

La Capa 3 de 5G, es decir, la RRC incluye las funcionalidades siguientes:

- Transmisión de información del sistema para NAS y AS.
- Establecimiento, mantenimiento y liberación de conexión RRC.
- Gestión de claves y otros procedimientos de Seguridad.
- Establecimiento, configuración, mantenimiento y liberación de portadores de Radio punto a Punto (PTP).
- Funciones de Movilidad.
- Mediciones o informes de la Interfaz de Radio desde el UE.

La Interfaz F1 se utiliza para dividir el gNB en dos componentes:

- La Unidad Central (gNB-CU).
- Y una o dos Unidades Distribuidas (gNB-DU).

Los protocolos RRC, PDCP y SDAP, se encuentran en el gNB-CU, mientras que RLC, MAC y PHY en gNB-DU (ver la Figura 45). [30]

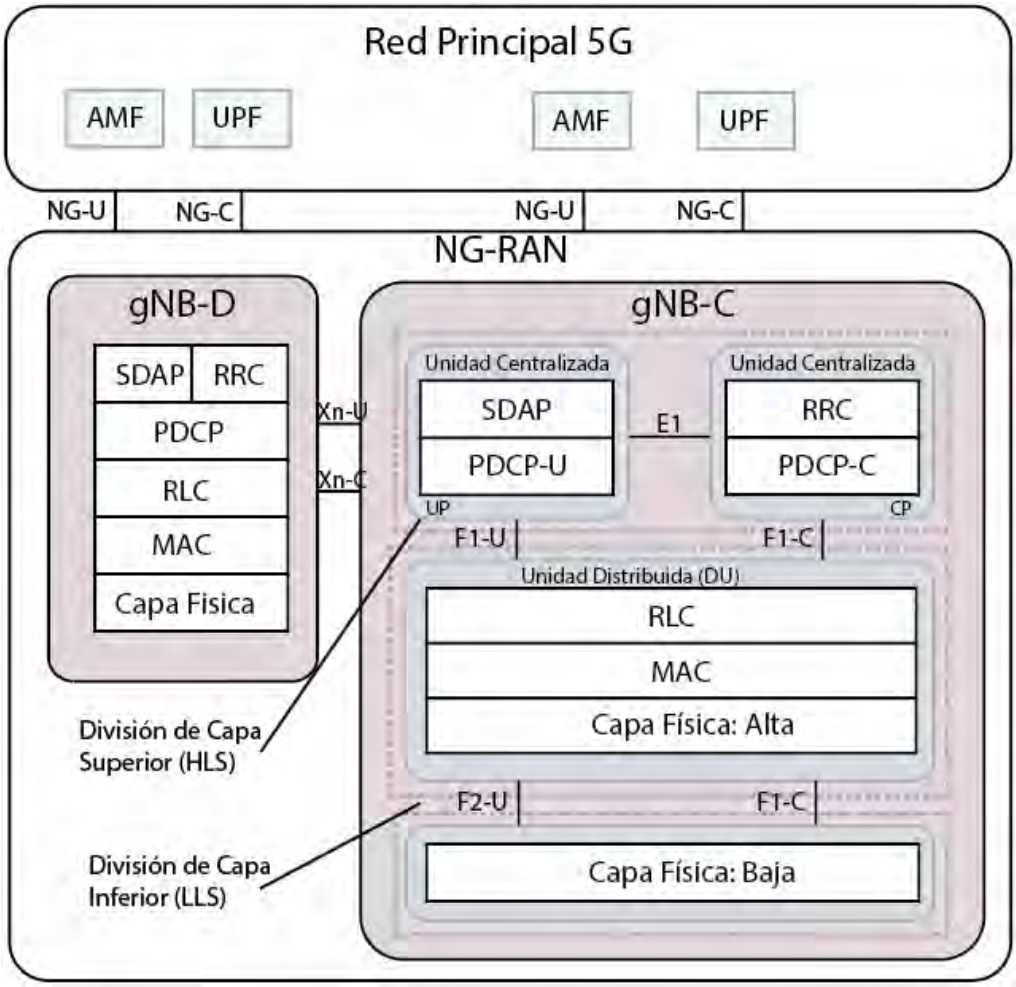


Figura 45 Protocolos en gNB-C y gNB-U. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

2.2.1.6.7 Segmentación 5G

La división de la Red brinda la posibilidad de aislar los recursos de la Red para ciertos servicios. El Sistema 5G puede ejecutar el aprovisionamiento de recursos para cierto conjunto de nodos de la Red lógica se asignen a u tercero, por ejemplo, un proveedor de servicio de telefonía le asigna Ancho de Banda específico, según lo requiere a un suscriptor de telefonía, una parte del espectro bajo una frecuencia. [18] *Para más información consulte página 125.*

(Véase la Figura 42,) un ejemplo de dicho principio al dedicar los recursos de la UPF, SMF y AMF dentro de un conjunto de segmentos de Red aislados para cada organización cooperante que depende de esos segmentos. [18]

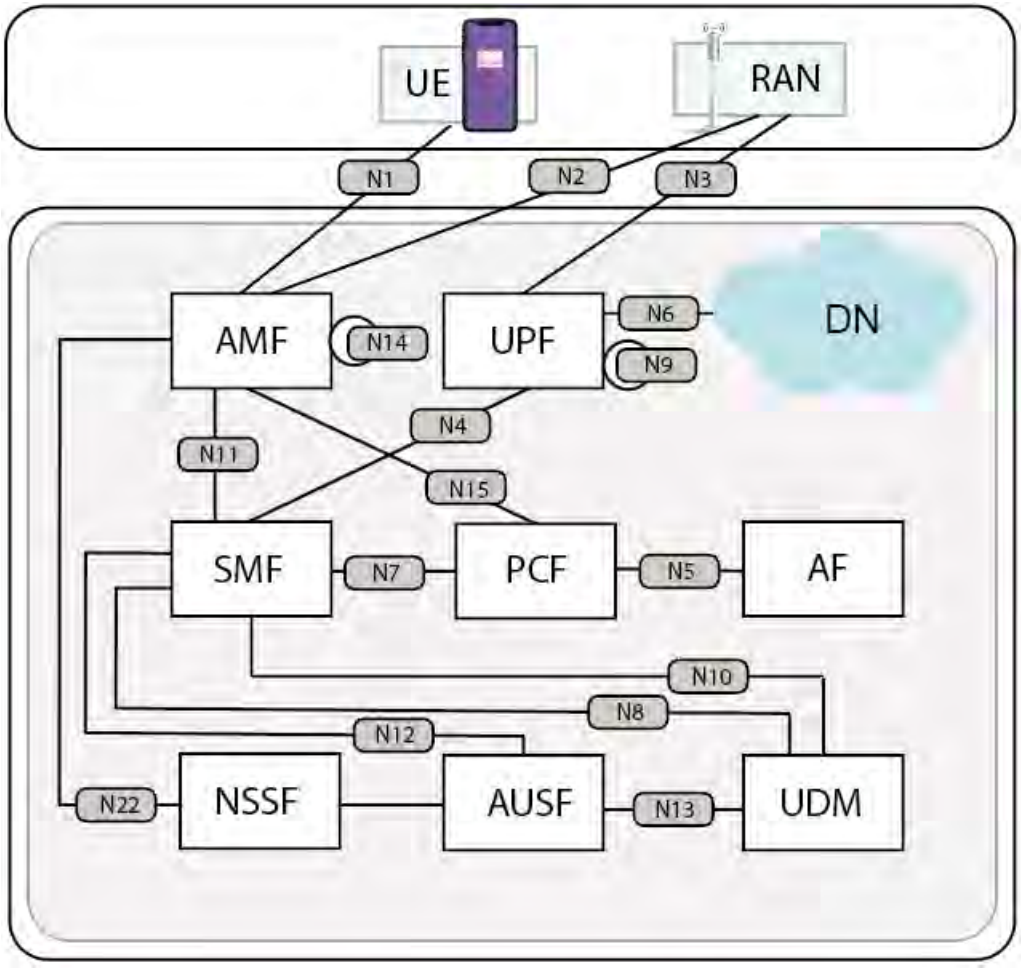


Figura 46 El principio de la Red dividida en el despliegue de la Red Central. Fuente: Jyrki T. J. Pennttinen (2019) [18]

2.2.1.6.8 Calidad de Servicio

5G no basta con ofrecer gran variedad de características y servicios, sino la manera que le hace frente a la variedad de recursos que se pueden utilizar al mismo tiempo o más rápido, sin perder de vista las necesidades del usuario, es eficaz.

El nivel de QoS de 5G se mide estableciendo requisitos indispensables por encima de las expectativas, en soporte, optimización, velocidad de datos, conectividad y mantenimiento, para garantizar el flujo de datos. [18]

2.2.1.7 Servicios TIC

Se encuentran en la página 129, 130 – 133 y 136 – 152.

2.3 Principales características 5G

Para lograr la conectividad 5G es necesario contar con una combinación de otras tecnologías, tales como Redes Heterogéneas (Helnet), MIMO, Ondas Milimétricas, comunicaciones D2D y M2.

5G no sólo establece una conexión de persona a persona usando Estaciones Móviles, como comúnmente se ha llevado a cabo con otras "G" Móviles, sino la conexión de todo con todo. [22] ¿Pero cuáles son sus características?

2.3.1 Requisitos por encima de 4G

2.3.1.1 Tasa de Datos muy altas en las Redes en tiempo real

"Proyectada de 1 a 10 Gbps en un aumento de casi 10 veces de la tasa de datos en comparación con las Redes 4G LTE que tienen una tasa máxima de 150 Mbps. *Véase la página 47 3GPP velocidad máxima de DL.* [32]

"La tasa de datos y latencia son dos métricas de evaluación impactantes para evaluar la calidad de experiencia del usuario en los sistemas de comunicación inalámbrica. Cuando se trata del desarrollo del sistema de próxima generación estas métricas son claves para satisfacer la calidad de la experiencia de usuario." [20]

2.3.1.2 Baja latencia de ida y vuelta de 1 ms

Siendo una reducción diez veces mayor que las tecnologías 4G tradicionales que tienen 10 ms. [32]

2.3.1.3 Requisitos de Ancho de Banda de Área de la Unidad

Muchos dispositivos se conectarán en un área específica con grandes requisitos de Ancho de Banda durante un periodo de tiempo más largo. [32]

2.3.1.4 Disponibilidad percibida muy alta

La visión 5G es hacer que la Red esté disponible para los dispositivos conectados casi todo el tiempo, teóricamente un 99.99%. [32]

2.3.1.5 Cobertura total independientemente de la ubicación

Las tecnologías 5G planean proporcionar una cobertura total a todos los dispositivos conectados en todo momento, independientemente de la ubicación de los dispositivos. [32]

2.3.1.6 Reducción de uso de energía

Debido al gran aumento en la velocidad de datos y los requisitos de conectividad, se refleja un alto consumo de energía y se realizan investigaciones para reducirlo. La llegada de la comunicación ecológica abrió una forma de reducir el uso de energía en casi un 90%. [32]

2.3.1.7 Mayor duración de batería

Debido a la reducción de energía de los dispositivos conectados con la ayuda de tecnologías ecológicas, la duración de la batería de los dispositivos ha aumentado bastante." [32]

2.3.1.8 Fiabilidad y alta disponibilidad

"La confiabilidad se refiere a la capacidad para garantizar la tasa de éxito en la transmisión de datos en diferentes condiciones dependiendo los diferentes casos de uso y servicios." [20] 5G ofrece conectividad en cualquier momento, con la capacidad de resistir ante posibles escenarios si interrupciones.

2.3.1.9 Eficiencia energética de costes y de espectro

Con una mejora 100 veces más en la eficiencia energética en comparación de 4G actual. [20]

"Las Redes 5G serán más complejas que contendrán múltiples capas de funciones, activos virtuales y físicos inclusive el uso óptimo del espectro, basados en SDN/NFV." [22]

2.3.2 Requisitos según la UIT-R en IMT-2020

El UIT-R considera ocho parámetros importantes para el IMT-2020 para 5G como requisitos clave o características de la Red 5G. [19]

Tabla 35 Áreas de aplicación par 5G. Fuente: Ulrick Trick (2021) [19]

Requisitos	Descripción
Velocidad máxima de datos	Por usuario o UE hasta 10 Gbps en condiciones especiales hasta 20 Gbps.
Latencia	Para RAN mínimo de 1 ms
Movilidad	Hasta 500 km / h
Densidad de conexión	Hasta 10x106 UE/Km2
Eficiencia energética	Para RAN 100 veces mejor que IMT-Advanced, es decir, el mismo consumo de energía
Eficiencia del espectro y Ancho de Banda	3 veces mayor que IMT - Advanced

2.3.2.1 Comparativa entre IMT 4G y 5G

(Véase la Figura 47,) hace una referencia de los requisitos antes mencionados.

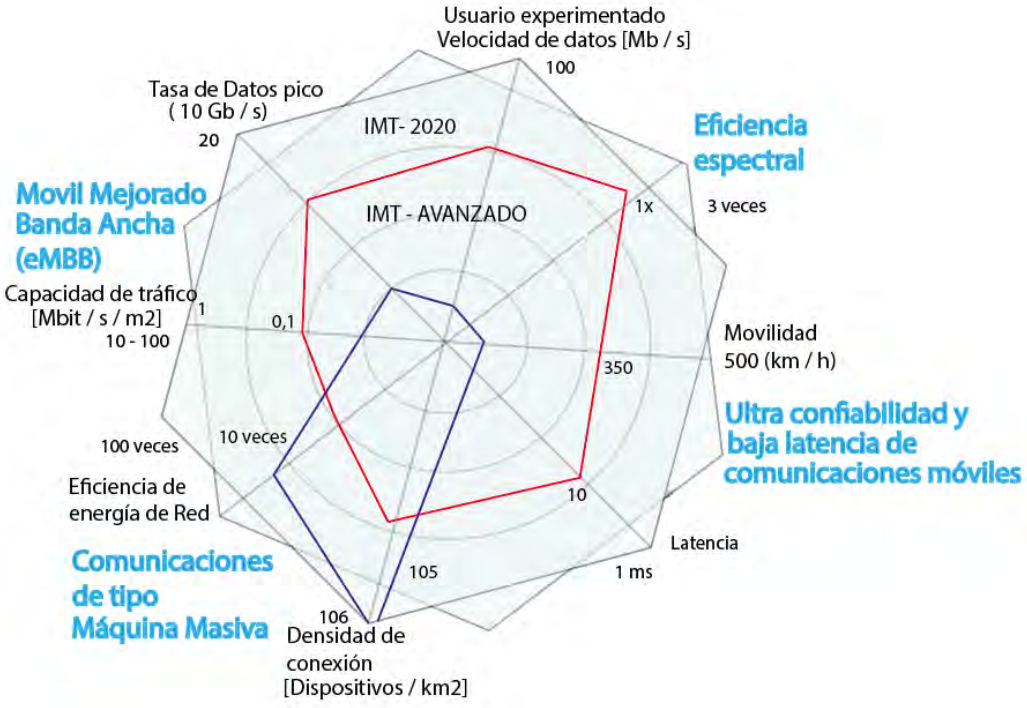


Figura 47 Brechas y desafíos 5G. Fuente: Carugi, Marco (2018) [42]

Para más información véase página 32 – 60 en el Marco de Referencia Capítulo 1.

2.3.3 Separación entre el Plano de Control y de Usuario

Véase tema "Arquitectura de Red de Acceso Radio (RAN) 5G" a partir de la página 91 hasta la 93.

La separación entre el Plano de Control y Usuario se ha usado desde 4G, pero para ser más específicos, el camino es más corto para tener mayor velocidad de conexión a comparación de generaciones anteriores.

2.3.4 Gran cantidad de dispositivos conectados

"La conectividad masiva se refiere al requisito de admitir un gran número de dispositivos conectados y, en consecuencia, un número grande de conexiones en una Unidad de Área. Con 5G el aumento exponencial o sólo proviene de la aparición de gran cantidad de tipos de dispositivos existentes, sino también de teléfonos inteligentes y tabletas." [20]

El valor esperado para esta métrica con 5G, es de decenas de GBps por kilómetro cuadrado. [20]

Tabla 36 Velocidades de referencia requeridas para uso de servicios tecnológicos 5G. Fuente: Plan Colombia (2019) [22]

Usos	Ancho de Banda requerido (Mbps)
Manufactura avanzada	38 – 74
Preparación para emergencias y seguridad	6 - 18
Educación y capacitación	38 - 74
Tecnologías de la salud	38 - 74
Redes limpias de energía y Transporte	2, 3
Uso de video interactivo en 3D	77, 148

2.3.5 Nuevas funciones y capacidades de infraestructura

2.3.5.1 Virtualización de Funciones de Red (NFV) disrupción del ecosistema de las TIC

Según la UIT-R (2018) “NFV se trata de implementar funciones de Red, programas que se ejecutan en la parte superior de la industria hardware estándar en lugar de un hardware dedicado (ver Figura 48).” [42] *El tema exclusivo se encuentra en la página 132.*

2.3.5.1.1 Beneficios de NFV

“Capex Opex reducidos. Por ejemplo, el consumo de energía.

2.3.5.1.2 Eficiencia incrementada

Varios inquilinos en una misma infraestructura.

2.3.5.1.3 Flexibilidad

Para proporcionar recursos en múltiples direcciones.

2.3.5.1.4 Agilidad

El tiempo de comercialización mejorado para incrementar nuevos servicios de Red.” [42]

Figura 48 Enfoque de dispositivos de Red Clásico y NFV. Fuente: UIT-R (2018) [42]

(Examine la Figura 50) se puede ver NFV y el tema se describe más adelante.

2.3.5.2 Edge Computing: recursos informáticos y almacenamiento junto con el usuario

2.3.5.2.1 Beneficios de Edge Computing

2.3.5.2.1.1 Latencia Ultra baja

"Mejora disruptiva de la experiencia del cliente.

2.3.5.2.1.2 Reducción del tráfico de la Red Central / Backhoul

Servicios en la nube, por ejemplo, Big Data cerca del usuario.

Véase la arquitectura de Edge Computing en la página 133, (ver Figura 52.)

2.3.5.2.1.3 Procesamiento dentro de la Red

Algunas cuestiones deben abordarse en su totalidad incluyendo la limitación de recursos, mayor complejidad, ejecución de aplicaciones, continuidad del servicio y movilidad." [42]

2.3.5.2.1.4 Una arquitectura funcional distribuida

Distribuciones de Red, aprovisionamiento de diversos servicios de Red mediante el uso de funciones de Red instanciadas en el lugar y momento adecuados." [42]

La organización de tal arquitectura se encuentra a partir de la página 83, juntamente con sus insumos, nodos hasta la página 98. Resumiendo, simplemente en el tipo de Acceso de Red, las funciones distribuidas de datos como AMF, SMF, división del Plano del Usuario y de Control, Calidad de Servicio, especificaciones de Control como la movilidad, control de sesiones, políticas, utilizando la Red de transporte para los datos, las funciones distribuidas de datos, incluyendo QoS, y los servicios que proporciona como el Internet y las aplicaciones [42]

“Este tipo de aprovisionamiento de diversos servicios de Red se da mediante el uso de Funciones de Red instanciadas en el lugar y momentos adecuados (ver Figura 49).” [42]

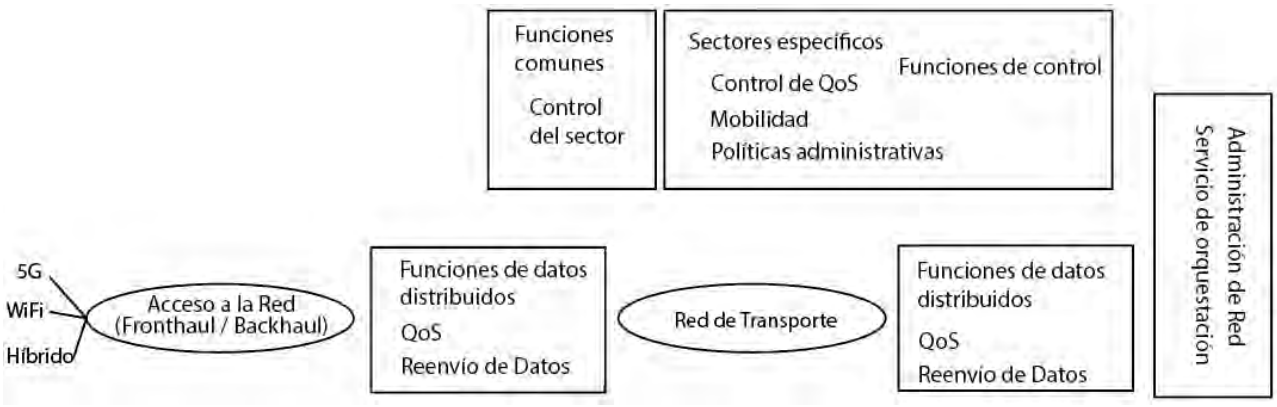


Figura 49 Arquitectura Funcional Distribuida. Fuente: Carugi, Marco (2018) [42]

2.3.5.3 Segmentación de Red: Soporte personalizado de aplicaciones

Este tipo de segmentación se encuentra en la página 117 – 118, es a través de Redes Lógicas dedicadas sobre una única Infraestructura, basándose en (la Figura 46), pero de manera adicional tenemos esta arquitectura usando instancias de segmentos de manera más proporcional (ver Figura 50). [42]

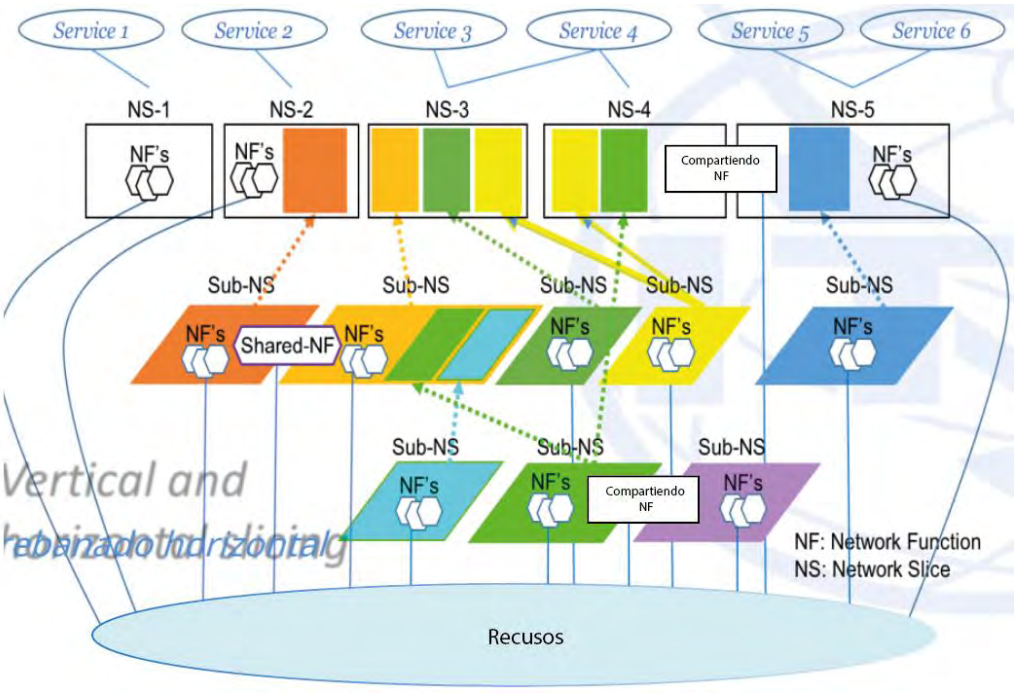


Figura 50 Corte de Red. Fuente: Carugi, Marco (2018) [42]

2.3.5.4 Redes de Acceso Heterogéneas y Red Central común

Las definiciones de Macro Celda, Pequeñas Celdas, Spot Cells como las mmWave, se encuentran en las páginas:

Organización Celular incluyendo Macro Celdas: páginas 16 – 18.

Pequeñas Celdas: páginas 85, 86

Arquitectura de Celdas Pequeñas: páginas 90, 91. (examine la Figura 37)

mmWave: página 104, 105.

2.3.5.5 Convergencia Móvil Fija 5G / IMT – 2020 (FMC)

Utilizando la arquitectura genérica que se encuentra en la página 89, Figura 31, la "Definición del Sistema Celular" en la página 12 y 13, (ver la Figura 49) "Arquitectura Funcional Distribuida": Una estación Móvil a través de una Interfaz de Radio se encuentra conectado con una Estación Base para establecer una comunicación con otro dispositivo, realizando una conmutación de la Red de llamadas de voz de Acceso Móvil, también puede utilizarse por ejemplo para tener Acceso a Internet, según la IMT – 2020 a través de las diversas modalidades de conexión, en este caso sería a través de un Punto de Acceso Inalámbrico, dentro del hogar. [42]

2.3.5.5.1 Motivaciones para la FMC

2.3.5.5.1.1 Desde la perspectiva del servicio

"Experiencia fluida y la disponibilidad de servicio ubicua.

- Carga unificada.
- Identidad de usuario de manera unificada y
- La continuidad de servicio.

2.3.5.5.1.2 Desde la perspectiva de la Red

Coordinación Mutua y evolución.

- Arquitectura de Red simplificada con funciones convergentes, operación flexible a través de la coordinación AN, uso compartido de recursos.
- Reducción de OPEX y CAPEX que son las funciones, datos de perfil de usuario comunes.” [42]

2.3.6 Habilitador para gran variedad de aplicaciones

Dos tercios de las categorías de casos de uso 5G, estarán relacionadas con la IoT y la comunicación de tipo máquina (MTC). [20] [42]

2.3.6.1 IoT

“IoT se refiere a un vasto conjunto de todo tipo de equipos conectados a Internet, incluidas cámaras de vigilancia, refrigeradores, impresoras, sensores, automóviles autónomos y dispositivos telemáticos que pueden comunicarse y realizar acciones.” [18]

La importancia de IoT es facilitar la vida del usuario a través de funciones útiles a través de Internet. “IoT ofrece una gran cantidad de nuevas posibilidades para administrar, coordinar, automatizar y beneficiarse de las comunicaciones M2M sin intervención humana, pero también se basa en interacciones humanas cuando es necesario. Conectándose a los objetos y base de datos para que forme parte de un entorno completo. [18]

2.3.6.1.1 Primeras implementaciones IoT

Las primeras implementaciones IoT se dieron cuando un grupo de estudiantes de la Universidad de Carnegie Mellon encontraron la manera de contar latas restantes de una máquina expendedora agregando un fotosensor al dispositivo cada vez que una lata salía, encontrando una forma de comunicación con la máquina y el mundo exterior. En otra ocasión

en el 2015 mediante un caso judicial, se dieron a conocer evidencias contundentes para poder enjuiciar a una mujer, utilizando datos FitBit. [8]

El primer vistazo de IoT actual fue a mediados del año 2000, cuando LG dio a conocer un refrigerador que funcionaba juntamente con una pantalla LCD usando el Internet, las funcionalidades además de lo habitual, con ayuda del LCD se podía ver la temperatura de manera digital, puntajes de frescura de los alimentos almacenados, la integración de una cámara web para evitar gastar recursos abriendo el refrigerador y monitorear los artículos desde el exterior. [8]

El primer dispositivo que probablemente llamó la atención de los medios fue el Nest Learning Thermostat en octubre del 2011. Este termostato programable, ha servido para ajustar las diferentes temperaturas de manera automática dentro del hogar usando Internet, según el horario del usuario, y así optimizar el uso de energía de otros recursos. [8]

La línea del tiempo del IoT y la creación de nuevos productos innovadores como dispositivos inteligentes o aplicaciones móviles que faciliten la comunicación entre dispositivo y persona, ha despertado el interés de los usuarios para poder adquirirlos y usarlos en la vida diaria. Hoy en día podemos utilizar sensores con movimiento, tener a nuestro alcance domótica en nuestro hogar como parte de nuestra evolución y reducir el tiempo que podemos ocuparlo en algo que realmente sea útil. [8]

2.3.6.1.2 Componentes de IoT

Entre los componentes tenemos:

2.3.6.1.2.1 Aplicación móvil

“Estos nos permiten controlar los dispositivos inteligentes: encender y apagar las luces, agregar nuevos dispositivos al sistema del hogar inteligente.” [8]

2.3.6.1.2.2 Panel de Control basado en Web

“Esto permite monitorear al dispositivo, ver información de uso, análisis, controlar los permisos, etc.” [8]

La mayoría de los dispositivos contarán con una Interfaz Web que administra su información. [8]

2.3.6.1.2.3 Interfaces de Red Inseguras

"Son los componentes del dispositivo IoT que están expuestos a través de la Red y podrían verse comprometidos debido a las vulnerabilidades en la Interfaz expuesta." [8]

2.3.6.1.2.4 Firmware

"Controla los diversos componentes del dispositivo y es responsable de todas sus acciones." [8]

Estos componentes en conjunto forman IoT que pueden ser utilizado en diferentes casos según las necesidades de los usuarios. [8]

2.3.6.1.3 Big Data

El conocimiento se duplica cada vez más por el número personas que realizan aportaciones cada vez más transitorias, con el Internet de las Cosas significa el incremento del conocimiento y la inmensa cantidad de datos que tendrá que transportar las redes de telecomunicaciones, el valor que tiene es infinito, por lo tanto, dales datos estarán expuestos a riesgos de Seguridad realmente serios. [22]

5G no sólo establece una conexión de persona a persona usando Estaciones Móviles, como comúnmente se ha llevado a cabo con otras "G" Móviles, sino la conexión de todo con todo, habilitando la Inteligencia de la Red, contando con infinidad de servicios disponibles, conectados a multitud de plataformas, protecciones o facilidades. "Cada individuo contará con una Red de Área Personal (PAN = Personal Área Network) conectada a una Red de Área Amplia o Global (WAN = Wide Área Network o GAN = Global Área Network) de manera ágil con ayuda de IPv6[53], facilitando que cada individuo sea una fuente inagotable de datos (Big Data) teniendo más libertad de uso. [22]

[53] "Direcciones IP Versión 6." [22]

Big Data de acuerdo con la capacidad de 5G, los Controladores, Sensores y Gateway para transportar datos tiene los siguientes desafíos según la IEEE 2018, de las cuáles son:

2.3.6.1.3.1 Datos en movimiento de alta velocidad

Por ejemplo, con automóviles autónomos, utiliza una gran cantidad de datos en movimiento de alta velocidad, IoT industrial a gran escala en Ciudades Inteligentes, generan zettabytes de datos en pocos minutos, necesitando un soporte avanzado de infraestructura para que pueda admitir la lectura y escritura ultrarrápida con arquitecturas robustas de almacenamiento. [22]

2.3.6.1.3.2 Soporte para inteligencia de aplicaciones y Red

El soporte de Big Data para el análisis y operabilidad de los casos de uso en Redes Distribuidas o la inteligencia de Aplicaciones requieren una arquitectura que pueda ser compatible y realmente pueda ser utilizado más allá con gran cantidad de datos con aplicaciones en tiempo real. [22]

2.3.6.1.3.3 Seguridad de extremo a extremo

Es fundamental la estructura de una arquitectura sólida y segura para las aplicaciones que requiere para el transporte inmenso de datos. [22]

2.3.6.1.3.4 Información procesable en tiempo real

Para las transferencias en tiempo real basado en la nube se necesita baja latencia como requisito esencial del 5G, así como el análisis de borde, vigilancia, atención de emergencia. [22]

2.3.6.1.4 Concepto de nube

5G como se ha dicho antes, es una tecnología innovadora, muy diferente a las demás generaciones, por lo tanto, ofrece mejores condiciones de uso, aplicaciones que requieren una

velocidad óptima. “El concepto de nube quiere decir que existe Inteligencia en la Red 5G, a su vez permite que los dispositivos de usuario se comuniquen de manera eficiente a través del transporte optimizado y funcionalidades centrales.” [18]

Esto quiere decir que se utiliza para optimizar la conectividad, latencia entre otras características de rendimiento esenciales, siendo redes flexibles en conjunto y escalables.

2.3.6.1.4.1 Red de Acceso por Radio Basado en la nube

“La Red de Acceso Basado en la nube (Cloud – RAN) es una solución ideal para diseñar la parte de Acceso de Radio de las Redes 5G, ya que permite la eficiencia energética, el ahorro de costos en los recursos de Banda Base, así como las mejoras de la capacidad de Red, mayor rendimiento, etc. Es esencialmente el desacoplamiento del Remote Radio Head “Cabezal de Radio Remoto (RRH) de la Unidad de Banda Base (BU) de una Estación Base y la implementación de BU en un entorno de computación e la nube. Los RRH se conectan a un grupo de BBU mediante el uso de redes frontales de enlace de microondas o fibra óptica de alta velocidad (ver Arquitectura en la Figura 51).“ [20]

2.3.6.1.4.2 Computación Móvil de borde y niebla

Muchos servicios y aplicaciones que ofrece la nueva generación móvil requieren de una latencia muy definida con gran capacidad de velocidad de datos. Para que pueda cubrir con los requisitos estrictos es llevar los servicios TIC y las capacidades de procesamiento al borde de la Red Móvil, dentro de la RAN y muy cerca de los usuarios móviles.

Mobile Edge Computing (MEC) se encarga de llevar ese procesamiento dentro de la RAN, ofreciendo al usuario una experiencia mejorada a comparación de otras generaciones, reduciendo la latencia y garantizando una eficiente operación de la Red sin retardos. [20]

Adicionalmente, las funciones de la Red Central 5G se realizarán como máquinas virtuales o contenedores controlados por el administrador de la nube. [20]

(Ver la Figura 52), en la página 133 la “Arquitectura Mobile Edge Computing” podemos ver la Arquitectura de Computación Mobile de borde y niebla.

2.3.6.1.4.3 Virtualización de la Red

NFV que es Virtualización de la Red permite reducir los gastos como una manera de ofrecer rentabilidad, teniendo un impacto en los ingresos de los operadores móviles. Por ejemplo, esperando que el costo de la implementación, gasto de capital (CAPEX) de operación, administración o gasto operacional (OPEX) sean muy bajos.

Según Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) NFV "se refiere a la reubicación de funciones de Red, que tradicionalmente se implementan en plataformas de hardware costosas y dedicadas a dispositivos de software que se ejecutan en el entorno de la nube o en servidores básicos de uso general. Al operar la función como software, es más fácil para los operadores móviles escalar más fácilmente los recursos de computación, almacenamiento y redes de acuerdo con las demandas de tráfico y para acelerar el tiempo de comercialización de nuevos servicios." [20]

(Examine la Figura 53) la Arquitectura en Bloques SDN utilizando Virtualización de la Red.

2.3.6.1.4.4 Comparativa Computación Móvil y NFV

"La computación en la nube nació para virtualizar el hardware de TI Básico, mientras que NFV se refiere a la inspiración de la computación de la nube para virtualizar las funciones de Red. Muchas funciones NFV como OpenStack o VMware sirven como backend de recursos para funciones de Red Virtual. [20]

2.3.6.1.5 Arquitecturas IoT

2.3.6.1.5.1 Arquitectura de concepto de nube

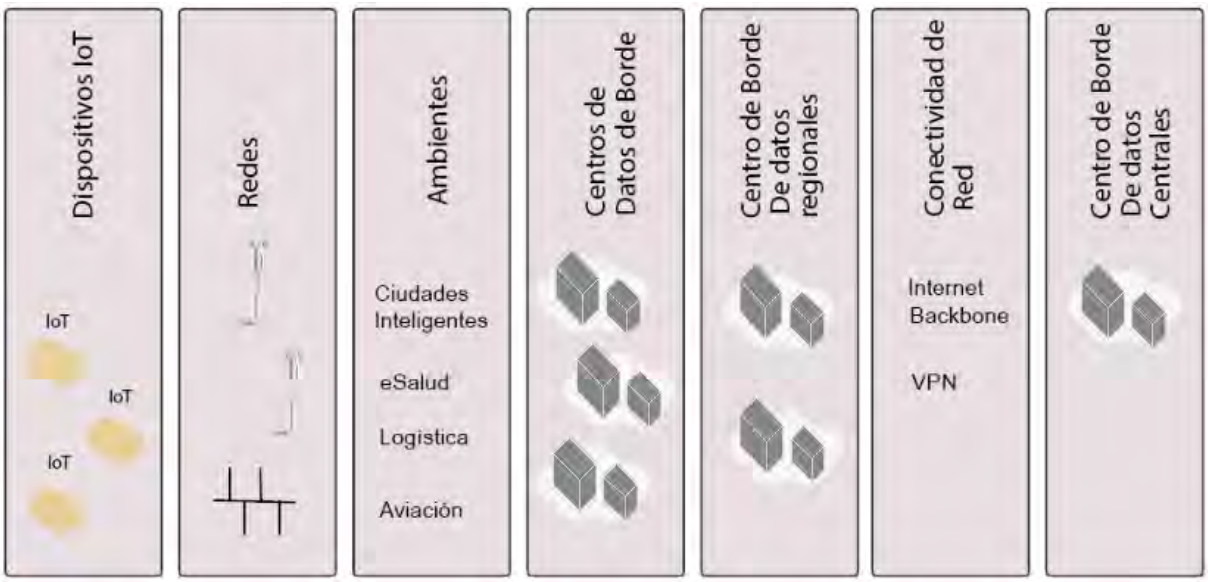


Figura 51 Un ejemplo de concepto de nube distribuida. Fuente: Jyrki T. J. Pennttinen (2019) [18]

2.3.6.1.5.2 Arquitectura de Computación Móvil de borde y niebla

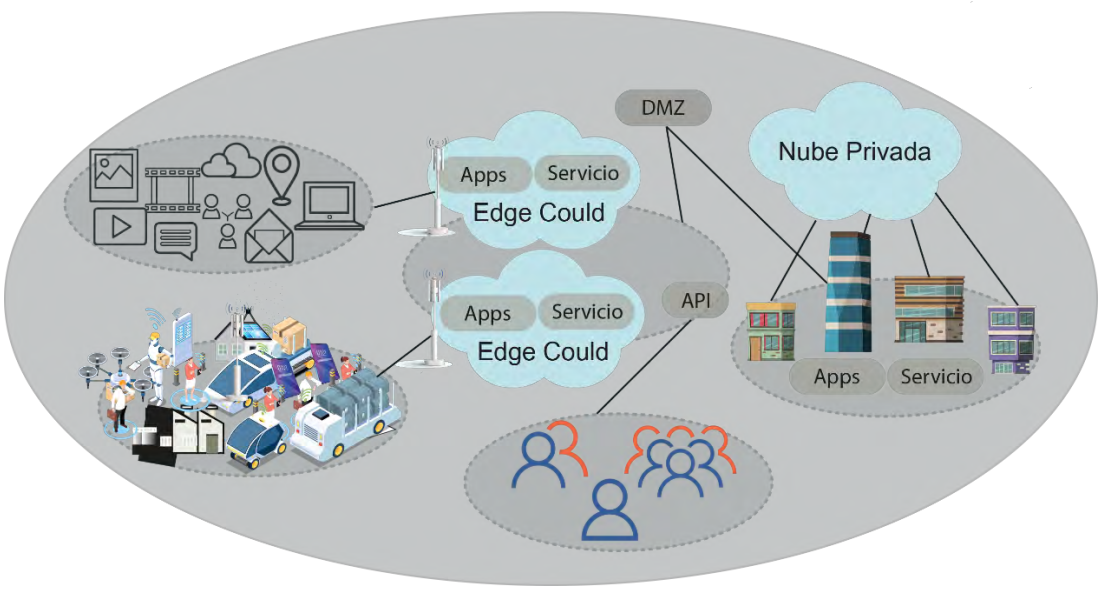


Figura 52 Arquitectura de Mobile Edge Computing. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov (2018) [20]

2.3.6.1.5.3 Arquitectura de NVF

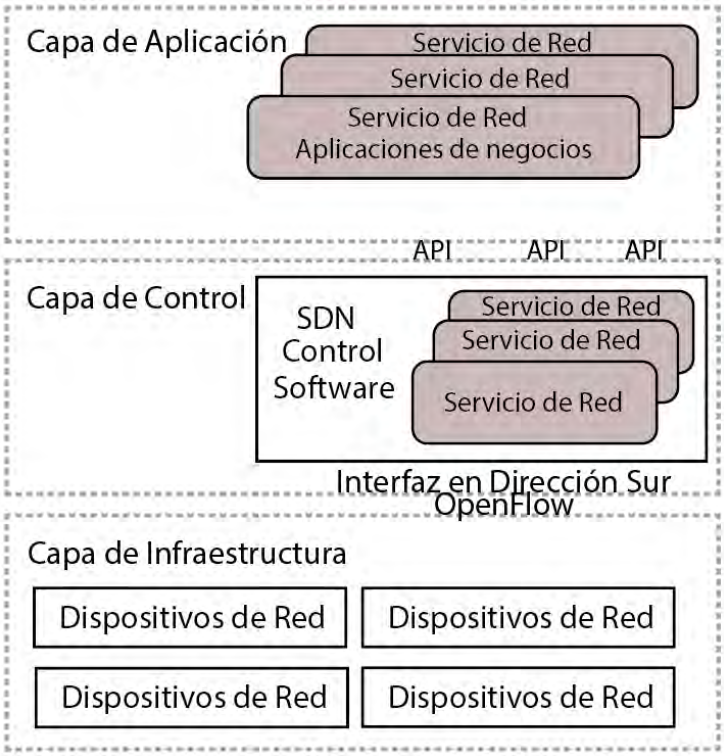


Figura 53 Arquitectura SDN utilizando Virtualización de la Red NFV. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) [20]

2.3.6.1.6 Estándares IoT

"IoT LPWA (Área Amplia de Baja Potencia) tiene dos subcategorías:

- Tecnologías LPWA para propiedades actuales, como el Acceso Múltiple de Fase Aleatoria (RPMA) de Ingenu, Sigfox y LoRa, Weightless, que operan con el espectro sin licencia y
- Tecnologías de IoT Celular (C-IoT) estandarizadas por 3GPP, que operan en un espectro con licencia, como NB – IoT, EC – GSM, etc." [18]

Examine la Tabla 37, la comparación de los Sistemas LPWA.

Tabla 37 Comparativa de los Sistemas LPWA. Fuente: Jyrki T. J. Pennttinen (2019 [18]

Variante LPWA	Estado
LoRa	La implementación de LoRa en NA ha presentado desafíos por las regulaciones de la FCC. El modo Híbrido lo resolvería.
Sigfox	Junio 2016: 100 ciudades de USA cubiertas por la Red Senet LoRa en California.
RPMA	Sigfox, se encuentra en proceso de implementación en 10 ciudades de USA: San Francisco, San José, California; Nueva York, Boston, Massachusetts; Atlanta, Georgia; Austin, Houston, Dallas, Chicago.
Basado en LTE	15 de Febrero del 2017: Ingenu se asoció con Microsoft para utilizar Microsoft Azure IoT Hub para facilitar la implementación IoT de un extremo a otro basado en RPMA. Azure IoT admite varios sistemas operativos y protocolos, lo que brinda a los desarrolladores en Sistemas IoT los medios para conectarse, monitorear y administrar los activos IoT. T-Mobile y Vadafone activos en implementaciones de NB-IoT en Europa. Huawei había anunciado que comercializará su marco y tecnologías NB-IoT a principios del 2017, incluido el lanzamiento de su procesador comercial System On a Chip. Sin embargo la empresa era poco conocida en América del Norte en ese entonces.

"La mayoría de las iniciativas basadas en NB – IoT se encuentran Lora en Japón, M1 en Singapur y KT Corea del Sur." [18]

2.3.6.1.6.1 3GPP

"3GPP para MNO ofrece soluciones para diversos mercados que incluye NB – IoT, eMTC, EC – GSM – IoT." [18]

2.3.6.1.6.1.1 LoRa

"LoRa Alliance crea estándares para IoT y promueve el creciente ecosistema para impulsar las implementaciones de volumen para redes de Área Amplia de Baja Potencia (LPWAN)." [18]

Según Jyrki T. J. Pennttinen (2019) LoRaWAN "es una especificación estandarizada por LoRa Alliance que incluye ST, Microchip y Amiho. Se basa en tecnología desarrollada por el proveedor de chipsets Semtech y hasta el 2018 estaba en fase de despliegue en Europa." [18]

Una de las características que definen los dispositivos LoRaWAN es su capacidad de implementarse en múltiples Redes y desplazarse de una Red a otra independientemente de la infraestructura de Red o del operador. [18]

"ETSI requiere que LoRa admita un mínimo de tres canales en 868,10 MHz, 868,30 MHz y 868,50 MHz." [18]

2.3.6.1.6.1.2 Ingenu

“Está construyendo la Machine Network, es decir, la Red IoT dedicada a la conectividad LPWA para máquinas. Diseñado para aplicaciones de bajo consumo, bajo costo y largo alcance donde la vida de la batería y la longevidad de la Red. [18]

2.3.6.1.6.1.3 Sigfox

Sigfox brinda soluciones económicas, confiables y de bajo consumo de energía basado en la conectividad IoT a través de Redes dedicadas. Sus requisitos generales incluyen simplicidad[54], solicitud de conexión y autonomía[55], dando como resultado activos óptimos o multimedia a través de la necesidad de simplemente pequeños mensajes. [18]

2.3.6.1.7 Casos de uso

2.3.6.1.7.1 Casos de uso generales

(Según la Figura 50,) en resumen se tiene la siguiente lista donde se muestra los diferentes casos de uso para Redes 5G de manera general. [19]

2.3.6.1.7.1.1 Fabricación

“Para el control remoto de movimiento y monitoreo de dispositivos como Robots, comunicaciones Máquina a Máquina, Realidad Aumentada (AR) y Realidad Virtual.

2.3.6.1.7.1.2 Automotriz

En cualquier tipo de comunicación, incluidos los camiones, actualizaciones de mapas a alta resolución, actualizaciones remotas y actualizaciones de software.

---

[54] “Sin necesidad de configuración.” [18]

[55] “consumo de energía extremadamente bajo que permite años de autonomía en una sola carga de batería.” [18]

2.3.6.1.7.1.3 Entretenimiento

Para la transmisión de video en UHD móvil de Ultra Alta definición.

2.3.6.1.7.1.4 Energía

Por ejemplo, para el control y monitorización de la Red, la conexión de parques eólicos, carga inteligente de vehículos eléctricos.

Figura 54 Casos de uso 5G. Fuente: Elaboración propia basado en [19]

2.3.6.1.7.1.5 Transporte público

En entrenamiento, operaciones de trenes o autobuses.

2.3.6.1.7.1.6 Agricultura

Para conectar sensores y máquinas agrícolas, control de drones.

2.3.6.1.7.1.7 Seguridad pública

Detención de amenazas, reconocimiento facial, control de drones.

2.3.6.1.7.1.8 Salud

Medicina bioelectrónica, sistemas de salud personal, telemedicina, cine, ambulancia conectada.

2.3.6.1.7.1.9 Megaciudades

Aplicaciones relacionadas con el control de misiones para la Seguridad Pública, la videovigilancia.” [19]

2.3.6.1.7.2 Caso de uso según la IMT

5G tiene una amplia variedad de casos de uso, de las cuales se encuentran definidos bajo la UIT-R en la IMT-2020, sintetizados en tres escenarios:

2.3.6.1.7.2.1 Banda Ancha Móvil Mejorada (eMMB)

Permite volúmenes de datos mayores y una experiencia de usuario mejorada. [15]

2.3.6.1.7.2.2 Comunicaciones Masivas de Tipo Máquina (mMTC)

La característica principal es una gran cantidad de dispositivos conectados de tipo máquina, teniendo transmisiones muy escasas de pequeños volúmenes de datos que no son sensibles a los retrasos. Por ejemplo, sensores remotos, actuadores y monitoreo de varios equipos. [15]

2.3.6.1.7.2.3 Comunicaciones Ultra Confiables de Baja Latencia (URLLC)

Cubre la comunicación centrada en humanos y máquinas. Por ejemplo, Seguridad del tráfico, control automático y la automatización de la fábrica. [15]

(Véase la Figura 35) "Arquitectura genérica para Sistemas Inalámbricos y 5G y MIMO Masivo" que se encuentra en la página 89 podemos ver los diferentes casos de uso para las tecnologías IoT. De igual manera (véase la Figura 54,) en la página 137.

2.3.6.1.7.3 Descripción y requisitos de casos de uso

Examine la Tabla 38, según NGMN, una de las organizaciones de estandarización 5G, demostró 14 categorías de aplicaciones y 24 casos de uso de esta Red, estas son algunas de las categorías, casos de uso con los requisitos de tasa de datos según su UL y DL, con requisitos de movilidad muy elevados, latencia muy baja, etc. [19]

Tabla 38 Casos de uso y categorías de NGMN. Fuente: Ulrick Trick (2021) [19]

		Requisitos			
Categoría	Casos de uso	Latencia, usario final Tasa de Datos	A fin	Movilidad	Latencia muy baja
Banda Ancha Acceso en áreas densas.	Video generalizado, servicios en la nube, sociedad densa.	DL: 300 Mbits / s UL: 50 Mbit / s	10 ms	0 - 100 km / h	200 - 200 / km2
Banda Ancha de Acceso Ultra Alto.	Oficina inteligente	DL: 1 Gbit / s UL: 500 Mbits / s	10 ms	Peatonal	75000 / km2
Acceso de Banda Ancha / multitud.	Video / foto HD, compartiendo.	DL: 25 Mbit / s UL: 50 Mbits / s	10 ms	Peatonal	150 000 / km2 30000 / estadio.
50 + Mbit / s En todas partes.	50 Mbits / s en todas partes.	DL: 50 Mbits / s UL: 25 Mbits / s	10 ms	0 - 120 km / h	400 / km2 suburbano 100 / km2 rural
Banda de Amplia Gama de bajo costo	Redes con costo ultrabajo.	DL: 10 Mbits / s UL: 10 Mbits / s	50 ms	0 - 50 km / h	16 (km2
Banda Móvil Amplia en comunicaciones de vehículos.	Trenes de alta velocidad, computación remota.	DL: 50 Mbits / s UL: 25 Mbits / s	10 ms	Hasta 500 mm por hora.	200 / km2 500 usuarios activos
MTC de Banda Ancha (M2M)	Vigilancia.	DL: 50 Mbits / s UL: 25 Mbits / s	10 ms	0 - 120 km / h	200 - 2500 / km2 Ancha (M2M)
Latencia Ultra Baja.	Internet táctil	DL: 50 Mbits / s UL: 25 Mbits / s	< 1 ms	Peatonal	no crítico
Latencia Ultra baja, alta confiabilidad Resilencia y aumento de tráfico.	Tráfico automático, Robots, objetivos remotos, cirugía remota, conducción colab.	DL: 10 Mbits / s	1 ms	0 - 120 km / h	no crítico
Largo alcance MTC baja potencia	Ropa con Redes de sensores.	DL: 10 kbits / s	- 1 ms	0 - 500 km / h	200000 / km2

Tabla 39 Categorías de uso de 3GPP. Fuente: Ulrick Trick (2021) [19]

Categoría	Requerimientos generales
eMBB (Banda Ancha Móvil mejorada)	- Velocidad de datos muy altas, hasta 10 Gbit / s por usuario - Baja latencia - Alta densidad de tráfico, Tbit / s / km2 -Alta densidad para UE, hasta 2500 UE / km2 - Movilidad de 0 a 500 km / h - Sin requisitos especiales de disponibilidad y precisoón de posición.
CriC (Comunicaciones Críticas) o URLLC (Comunicaciones Ultra fiables y de Baja Latencia)	- Sin requisitos especiales para la velocidad de datos y la movilidad. - Latencia muy baja, < 1 ms de un extremo a otro. - Fiabilidad ultra alta, alta disponibilidad. - Alta densidad, <1000 UE por ejemplo sensores - Posición precisa <= 10 cm
MIoT Internet Masivo de las Cosas o mMTC (Comunicaciones de tipo Máquina Masiva)	- Sin requisitos especiales de velocidad de datos, latencia, confiabilidad y movilidad. - Comunicación eficiente para soportar dispositivos con recursos limitados, fuentes y suministro de batería de baja potencia. - Densidad muy alta, hasta 1 ms - Alta precisión de posicionamiento hasta 50 cm

En la Tabla 39 se define según el lanzamiento 14 de 3GPP 74 casos de uso en cinco categorías:

2.3.6.1.7.3.1 eMMB

"Por ejemplo televisión UHD, holograma, realidad aumentada, Realidad Virtual, presencia virtual, alta movilidad en trenes.

2.3.6.1.7.3.2 Comunicaciones críticas (CriC)

Como juegos interactivos, retransmisiones deportivas, drones, robots.

2.3.6.1.7.3.3 Comunicaciones masivas de tipo máquina (mTC)

Internet Masivo de las Cosas (MIoT) como casos de uso en metro o estadio, ciudades inteligentes (eCity), agricultura Inteligente (eFarm), control de inventario.

2.3.6.1.7.3.4 Operación de Red

Por ejemplo, Corte de Red o Segmentación, enrutamiento, migración y interfuncionamiento y ahorro de energía.

2.3.6.1.7.3.5 Mejora de comunicación V2X

En la conducción automática.” [19]

2.3.6.1.7.3.6 Banda Ancha Móvil Mejorada (eMMB)

2.3.6.1.7.3.6.1 Comunicaciones D2D

Se refiere a la comunicación directa entre dos usuarios y dispositivos móviles, sin atravesar una infraestructura de Red. La comunicación D2D puede mejorar la eficiencia del espectro, la ganancia de la velocidad de datos de usuario y reducir la latencia, como el consumo de energía. [20]

2.3.6.1.7.3.7 Comunicaciones Masivas de Tipo Máquina (mMTC)

2.3.6.1.7.3.7.1 Comunicaciones M2M

“La comunicación M2M, se refiere a las comunicaciones de datos automatizadas entre dispositivos y la infraestructura de transporte de datos subyacentes.” [20] Es decir, las comunicaciones de datos entre la M2M que se refiere a la comunicación de tipo máquina (MTC) y un servidor. [18]

Hay una serie de servicios y aplicaciones habilitados para este tipo de comunicación como puede ser la automatización del hogar, el monitoreo y medición, atención médica y automotriz, etc. [20]

2.3.6.1.7.3.7.2 Inteligencia Artificial (Machine Learning) y Ciudades Inteligentes

El espectro de aplicaciones 5G es muy amplio, pero se prevé que IoT de cuarta generación será uno de los motivadores más importantes para aplicaciones 5G, siendo Machine Learning una parte integral de la infraestructura 5G y Ciudades Inteligentes en conjunto. [22]

Véase las páginas 89 y 91, (Figuras 35 y 37,) ejemplos de una Arquitectura de Ciudad Inteligente.

Machine Learning en contexto subyacente brindará Redes más inteligentes para brindarle al suscriptor individual un mejor flujo de datos e información clave para la toma de decisiones. [22]

2.3.6.1.7.3.8 Comunicaciones Ultra Confiables de Baja Latencia (URLLC)

2.3.6.1.7.3.8.1 Vehículos Autónomos

La comunicación vehicular es uno de los pilares más importantes del 5G con una plataforma optimizada con múltiples beneficios, por ejemplo, para mejorar la Seguridad de los conductores y pasajeros o brindar apoyo para el manejo inteligente del tráfico, permitir que se puedan tomar decisiones factibles y apoyar la modernización de diferentes operaciones de vehículos junto con aplicaciones útiles para los usuarios (ver Figura 55). [18][32] Proporcionan una conectividad de Red robusta para transferir una gran cantidad de datos entre vehículos e infraestructuras relacionadas con la gestión del tráfico. [32]

La conectividad basada en celulares, especialmente con 3GPP LTE se está volviendo más factible también para las comunicaciones de vehículos locales, junto con la estandarización adicional, por ejemplo, comunicaciones directas entre dispositivos de usuario. [18] 5GAA (5G Automotive Association) es una iniciativa bastante nueva para impulsar la conectividad Celular en un entorno V2X. [18]

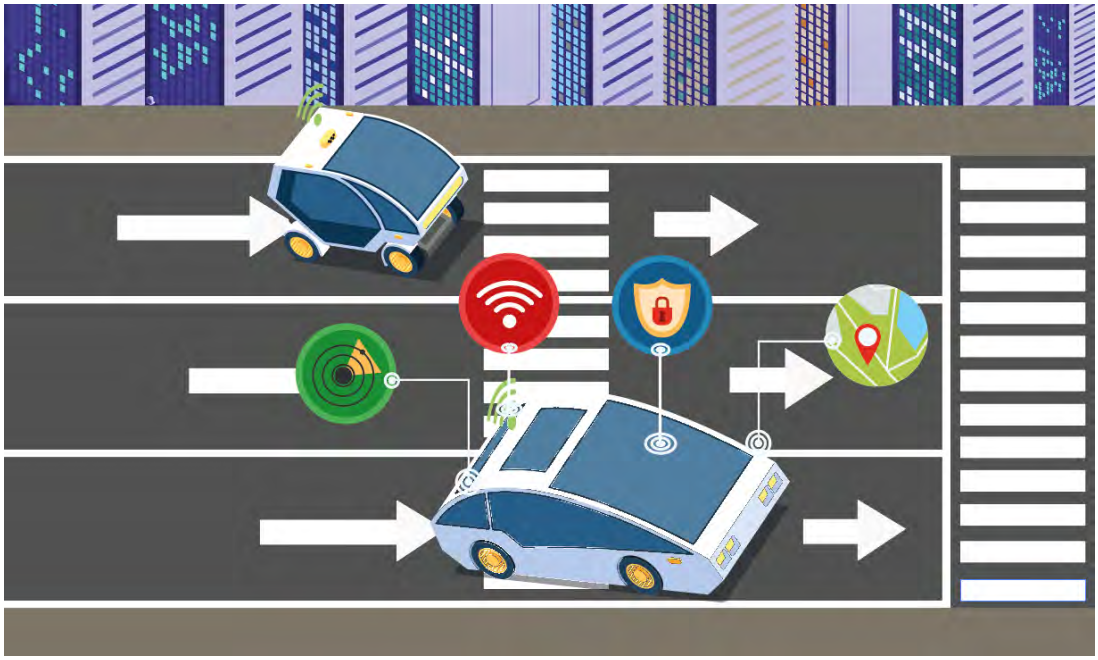


Figura 55 Aplicaciones vehiculares. Fuente: Elaboración propia basado en [32]

2.3.6.1.7.3.8.1.1 Funcionamiento

Se espera que los Sistemas de Transporte Inteligente (ITS) sean parte integral de las próximas sociedades desarrolladas, [32] su comunicación se basa en la WLAN IEEE 802.11p a 5,9 GHz en Europa y Estados Unidos. Cuando dos Estaciones ITS aparecen dentro del patrón de radiación de la antena principal se conectan automáticamente y establece una Red Ad-hoc donde las Estaciones ITS conocen su velocidad, posición proporcionando mensajes entre sí, sobre avisos o advertencias. Cada vehículo funciona como enrutador y puede enviar los mensajes a través de múltiples saltos a otros vehículos y Estaciones ITS. [18]

Los conductores cuentan con el apoyo de C-IST, que es un Sistema de Transporte Inteligente Cooperativo encargado de enviar advertencias utilizado aplicaciones, por ejemplo, de vehículo a vehículo incluye la advertencia de colisión frontal, punto ciego, cambio de carril, luz de freno de emergencia, pérdida de control y de no rebasar. [18]

2.3.6.1.7.3.8.1.2 Desafíos de despliegue

En general, las barreras que están frenando el despliegue de vehículos totalmente autónomos en las carreteras, son:

- El precio de los componentes tecnológicos sofisticados. [32]
- Confianza del consumidor en la tecnología de automatización. [32]
- Falta de regulaciones bien definidas. [32]

“Para cumplir con los requisitos de comunicación de vehículos, las comunicaciones vehiculares se pueden realizar en las Redes Celulares minimizando el costo de transmisión.” [32]

2.3.6.1.7.3.8.1.3 Necesidades de comunicación vehicular

Hoy en día las muertes por accidentes de tráfico sobrepasan el número en pandemias o desastres naturales, por lo tanto, es un número importante, lo cual la comunicación vehicular es esencial para reducir esa cantidad. Existen diferentes factores que podrían contribuir a los accidentes, por ejemplo, el 90% de los casos son causados por el conductor, donde podrían evitarse si dispusieran de una advertencia previa, en otros casos por infraestructura que se manipula de manera manual como la luz de freno trasera del vehículo que va adelante para elegir su actividad de frenado, limitando a los conductores en caso de emergencia, inclusive los retardos en las comunicaciones de alertas en crisis son excesivos. [32]

Los choques pueden evitarse, tomar el camino más corto de manera automática reduce el tiempo que se puede invertir en algo más y no limitarse a lo convencional. Actualmente gastamos nuestro tiempo en acciones vánales, cuando podríamos ocuparlo en nuestra familia, pero contar con este servicio reduce tiempo y complicaciones. [32]

2.3.6.1.7.3.8.1.4 Desafíos en las comunicaciones vehiculares

Entre los desafíos de las comunicaciones vehiculares se pueden encontrar:

- Las mezclas de las diferentes formas de comunicación por ejemplo en comunicaciones V2V, V2I, y V2P, generando problemas de compatibilidad. [32]
- Las entidades comunicantes que pueden ser estáticas o móviles, afectando significativamente el rendimiento. [32]

2.3.6.1.7.3.8.1.5 Tipos de comunicaciones vehiculares

2.3.6.1.7.3.8.1.5.1 V2V Comunicación de Vehículo con Vehículo

"La comunicación V2V es la transmisión inalámbrica de datos entre vehículos." [41]

Los vehículos autónomos son capaces de interactuar con vehículos cercanos, evitando accidentes, dependiendo de la correspondencia de datos al recibir y enviar las alertas, avisando a los conductores sobre las circunstancias de crisis que se podrían presentar y provocar un accidente. [32]

Por ejemplo, enviar alertas a los conductores sobre un posible choque masivo cercano por las fuertes nevadas en Nueva York, evita tomar la misma ruta que cientos de automóviles, mientras frena y retrocede, este vehículo al mismo tiempo avisa a los vehículos próximos que tengan cuidado porque está retrocediendo.

Para dar una mejor idea, se presenta la siguiente Figura (ver Figura 56), donde un vehículo emite señales de alerta a los vehículos cercanos, informando que está retrocediendo.

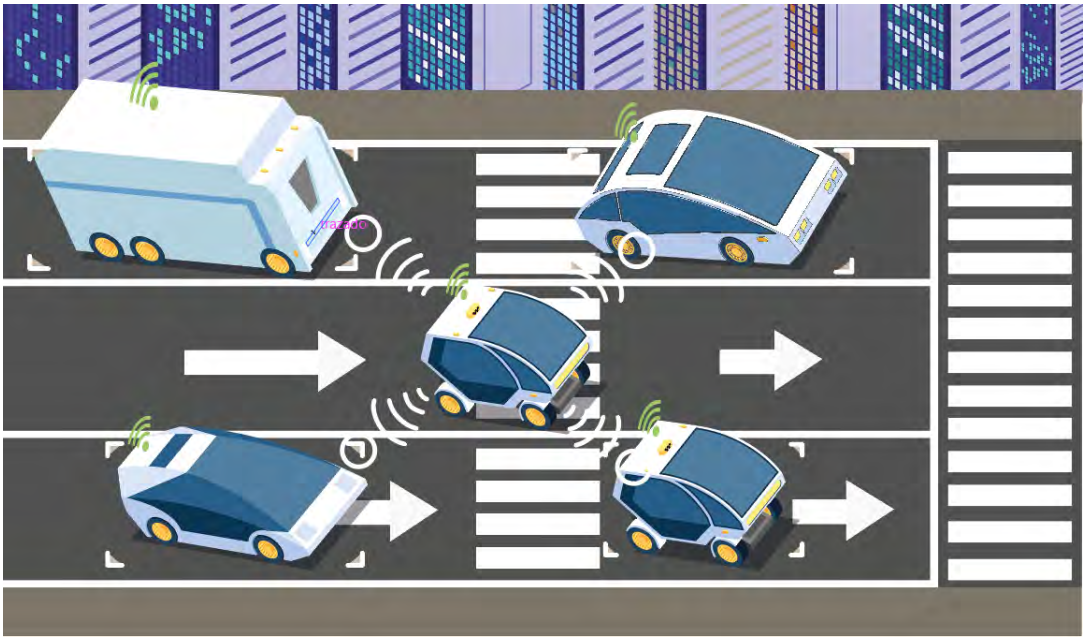


Figura 56 Comunicación V2V. Fuente: Elaboración propia basado en [32]

2.3.6.1.7.3.8.1.5.1.1 Composición V2V

Un sistema V2V comprende de 3 dominios distintos:

2.3.6.1.7.3.8.1.5.1.1.1 En el vehículo

Comprende de una Red compuesta por AU que son las Unidades de Aplicación y por una Unidad a Bordo (OBU). AU es un dispositivo dedicado que ejecuta una sola aplicación o un conjunto de aplicaciones, utilizando las capacidades de comunicación de la OBU. Este puede ser una computadora o una Estación Móvil estableciendo una conexión por cable, bluetooth o inalámbrica. [18]

2.3.6.1.7.3.8.1.5.1.1.2 Ad-hoc

"También llamado VANET[56] se compone por vehículos equipados con OBU y Unidades Estacionarias a lo largo de la carretera, es decir, Unidades de Carretera (RSU[57]). La OBU está equipada con un dispositivo de comunicación inalámbrica de corto alcance dedicado a la Seguridad vial. [18]

Las OBU forman una Red Ad-hoc Móvil llamado MANET para las comunicaciones entre nodos de manera distribuida sin la necesidad de una instancia de coordinación centralizada. [18]

2.3.6.1.7.3.8.1.5.1.1.3 Dominio de infraestructura

RSU para el acceso a Internet a menudo se configuran con un proceso controlado llamado C2C CC, es decir, Consorcio de Comunicación de V2V. Los puntos de acceso público o privados HS generalmente se configuran en ambientes menos controlados. [18]

Las RSU y HS no brindan acceso a Internet, pero "las OBU pueden utilizar las capacidades de comunicación de las Redes de Radio Celular (2G, 3G, 4G, 5G) si se encuentran integradas en la OBU. [18]

2.3.6.1.7.3.8.1.5.1.2 Posibles comunicaciones V2V

[56] "Red Ad-hoc Vehicular." [18]

[57] Antena.

2.3.6.1.7.3.8.1.5.1.2.1 Propagación de alertas por V2V

(Véase en la Figura 56) el ejemplo de prevención de un choque masivo.

2.3.6.1.7.3.8.1.5.1.2.2 Comunicación en grupo V2V

Varios vehículos forman un grupo y pueden comunicarse entre ellos, compartiendo información sobre el estado de los vehículos, contribuyendo una conducción segura. [41]

2.3.6.1.7.3.8.1.5.1.2.3 Balizaje V2V

Cada vehículo envía periódicamente la información sobre su propio estado, su dirección actual, la posición, entre otros. [41]

2.3.6.1.7.3.8.1.5.2 V2I Comunicación de Vehículo con Infraestructura

La comunicación V2I permite la comunicación de Vehículos con alguna infraestructura que se encuentre a las orillas de la carretera. [32]

2.3.6.1.7.3.8.1.5.2.1 Componentes V2I

Los componentes utilizados para admitir ese tipo de escenario incluyen los semáforos, las cámaras de las carreteras, marcadores de carril, luces de la calle y notas de estacionamiento. La fuerza V2I es evidente simplemente porque los avisos se mandan en tiempo real independientemente de las condiciones del tráfico. [32]

Hay diversos escenarios que de acuerdo con la adquisición de datos mediante sensores robustos se pueden comunicar como la congestión del tráfico, la disponibilidad del estacionamiento cercano y las áreas que son propensas a provocar algún tipo de accidente. Con esto se puede lograr la disminución de velocidad variable entre automóviles cercanos, tiempo de la señal, lo que permite el ahorro de combustible ya sea para elegir una mejor ruta factible o simplemente con la disminución de tráfico en la zona. [32]

“Estos avisos se pueden comunicar a los operadores de vehículos mediante pantallas en la carretera o mediante conexiones inalámbricas.” [32]

(La Figura 53) enfatiza que la infraestructura V2I cambia en condiciones cambiantes de tráfico.

“Las Unidades de Carretera RSU proporcionan cobertura de Red a los Vehículos de las carreteras. Un grupo RSU cercanas está conectado a Internet y otras Unidades de Control a través de Puertas de Enlace RSU.” [32] Para proporcionar una conectividad de Red fluida incluso a velocidades más altas, se emplean técnicas de transferencia suave. [32]

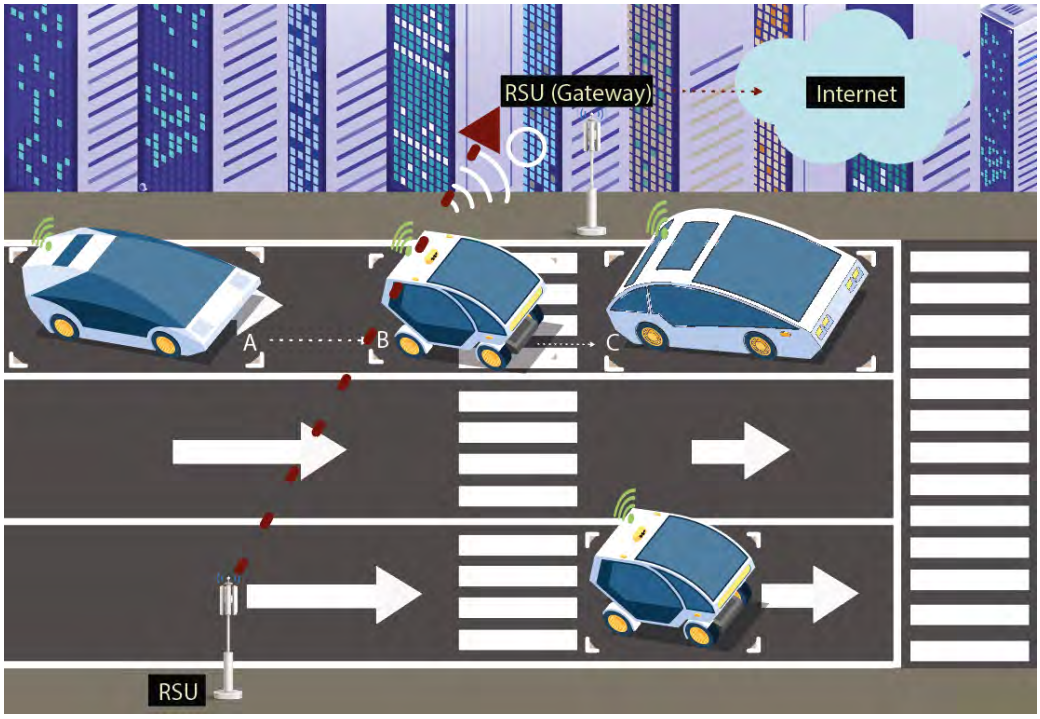


Figura 57 Comunicación V2I. Fuente: Elaboración propia basado en [32]

2.3.6.1.7.3.8.1.5.2.2 Posibles comunicaciones V2I

2.3.6.1.7.3.8.1.5.2.2.1 Alerta V2I

Permite las comunicaciones con RSU que es una infraestructura, en caso de accidente en una intersección una RSU puede enviar el mensaje de alerta a los vehículos que se acercan a la intersección. [41]

2.3.6.1.7.3.8.1.5.3 V2D / V2P Comunicación Vehiculares con Peatón (Dispositivo Móvil)

Uno de los seres más vulnerables son los peatones en los escenarios de colisión de vehículos (ver Figura 58). Existe un porcentaje considerable de accidentes dentro de colisiones, donde los ciclistas y peatones suelen ser alcanzados, provocando lesiones o la muerte. El propósito es detener a tiempo los vehículos antes de posibles choques, proporcionado advertencias de colisión. [32]

“El Teléfono Móvil frecuentemente ha sido una distracción para los conductores, inclusive peatones mientras cruzan la calle, así que se sugiere la solución de este problema a través de Telefonía Móvil. El concepto puede percibirse como el reemplazo de un dispositivo de comunicación de mano convencional por Teléfonos Inteligentes compatibles.” [32]

Figura 58 Comunicación V2D. Fuente: Elaboración propia basado en [32]

La tecnología WLAN y WiFi se puede utilizar para establecer un enlace entre la comunicación del vehículo con el peatón. [32]

2.3.6.1.7.3.8.1.5.3.1 Tipos de comunicación V2P / V2D

2.3.6.1.7.3.8.1.5.3.1.1 Comunicación V2P por enlaces directos

"Cuando se recurre a equipos terceros como puntos de acceso y encaminadores para comunicar un nodo con otro." [41]

2.3.6.1.7.3.8.1.5.3.1.2 Comunicación V2P por enlaces indirectos

"Cuando la comunicación de Vehículos con dispositivos nómadas se puede dar mediante enlaces directos sin intervención externa entre ellos o utilizando tecnologías de comunicación inalámbrica como Bluetooth, ZigBee y comunicación en un campo cercano." [41]

2.3.6.1.7.3.8.1.5.4 V2N Comunicaciones vehiculares a Red

"Los vehículos son capaces de realizar comunicaciones a través de la Red Centralizada para diferentes servicios de aplicaciones V2X. [32]

En la siguiente Figura (ver Figura 59,) el nodo de retransmisión móvil establece un enlace de comunicación entre Vehículo Móvil y Estación Base Vehicular utilizando una Red Celular." [32]

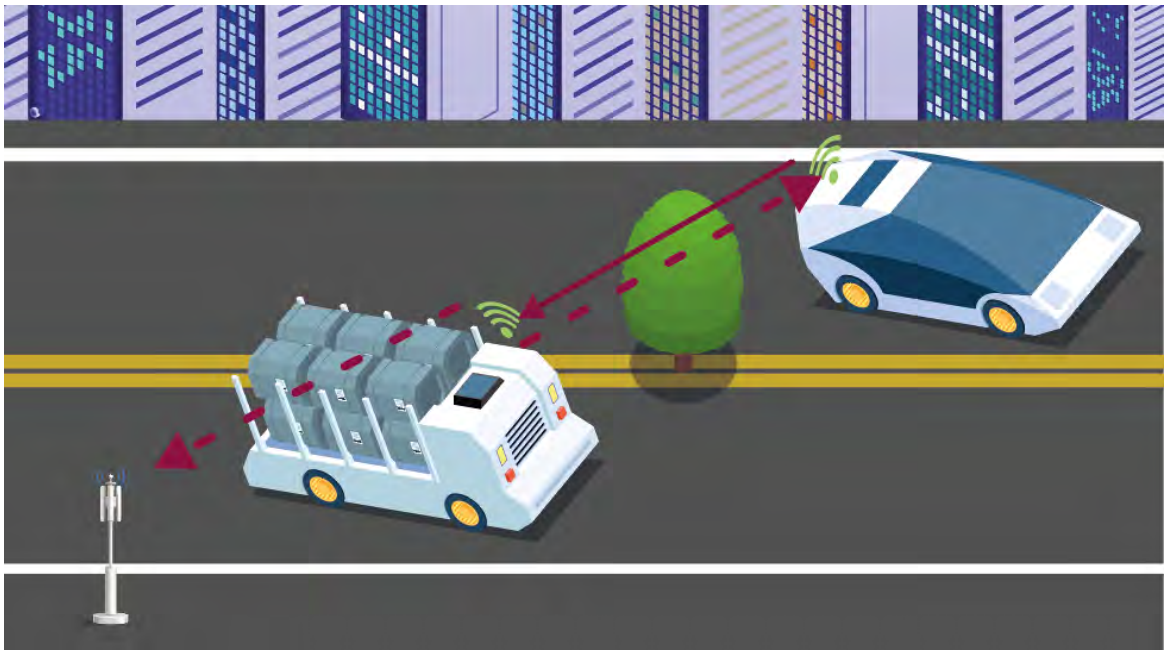


Figura 59 V2X Comunicación Vehicular con todo. Fuente: Elaboración propia basado en [32]

V2X se basan tradicionalmente en la conectividad IEEE 802.11p, de tal manera que tanto los vehículos como los elementos de la carretera establecen automáticamente la transmisión de datos en una Red Ad-hoc. [18]

5GAAA enfatiza el rendimiento mejorado en comunicaciones dedicadas a corto alcance basados en LTE sobre una variante de IEEE. Entre los beneficios de C-V2X incluyen:

- La codificación turbo frente a la codificación convolucional proporciona una ganancia de 3dB, lo que beneficia el presupuesto de Enlace de Radio. [18]
- Multiplexación por División de Frecuencia de Portadora Única (SC-FDM) frente a la multiplexación por División de Frecuencia Ortogonal (OFDM) optimizando la frecuencia de amplificador de potencia. [18]

2.3.6.1.7.3.8.1.6 Arquitectura

2.3.6.1.7.3.8.1.6.1 Arquitectura de los diferentes tipos de comunicaciones vehiculares

(Ver Figura 60)

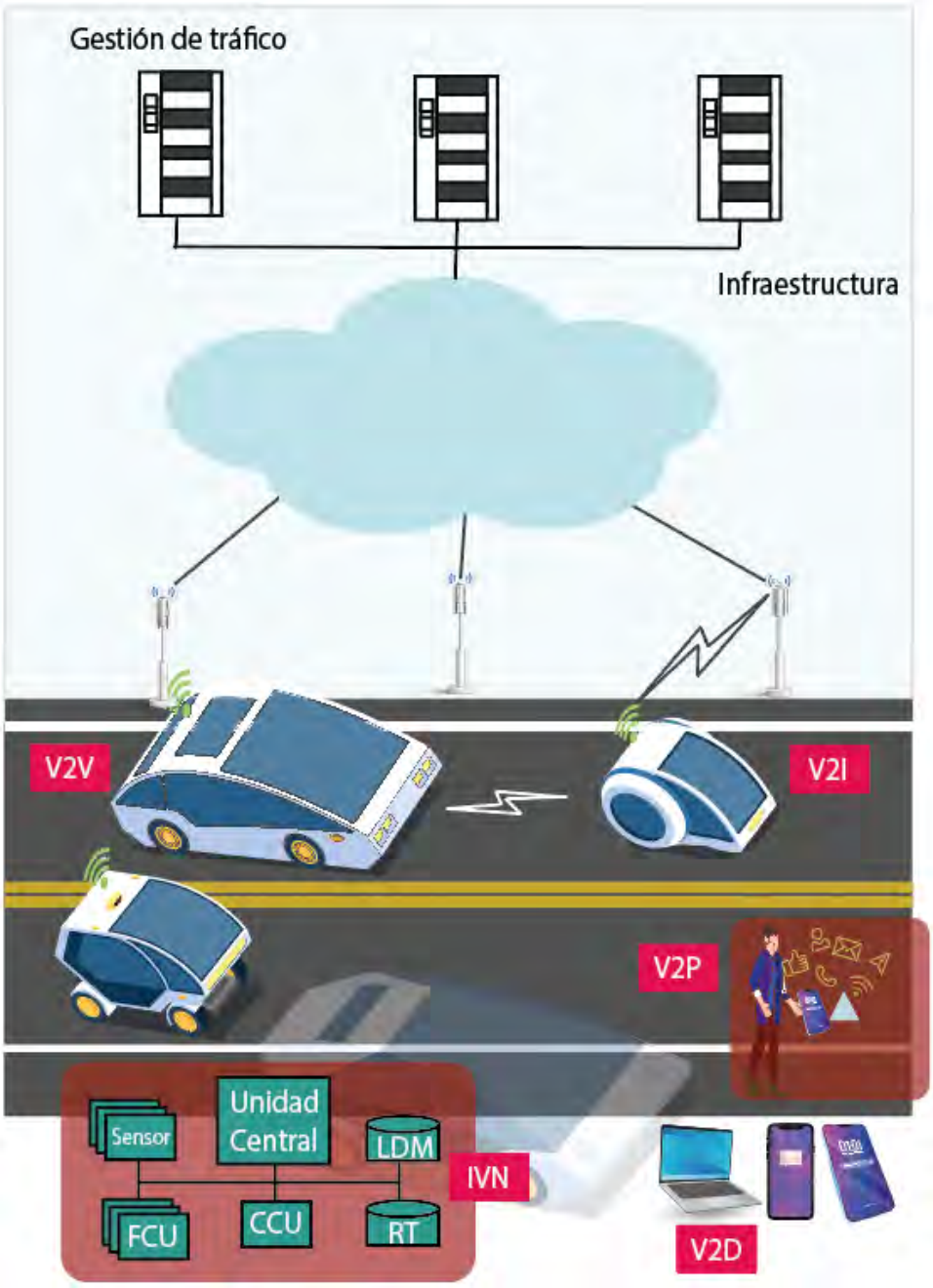


Figura 60 Visión general de la comunicación vehicular. Fuente UI-T (2020) [41]

2.3.6.1.7.3.8.1.7 Estándares vehiculares

2.3.6.1.7.3.8.1.7.1 3GPP

2.3.6.1.7.3.8.1.7.1.1 3GPP TR 22.886

“Especificación de 3GPP que define la solución de velocidades más cortas entre vehículos, reducir el consumo de combustible y reducir la conducción automatizada.” [14]

2.3.6.1.7.3.8.1.7.2 IEEE

2.3.6.1.7.3.8.1.7.2.1 IEEE 802.11p

“Es una enmienda aprobada por el estándar IEEE 802.11 y agrega un sistema de comunicación vehicular, es decir, al acceso inalámbrico en entornos vehiculares (WAVE) Define las mejoras de IEEE 802.11 necesarias para admitir el intercambio de datos de alta velocidad entre vehículos y V2I, utilizando una Banda con licencia de 5,9 GHz.” [14]

2.3.6.1.7.3.8.1.7.2.2 IEEE 1609

“Definen la arquitectura, los protocolos de Seguridad las funciones de gestión y un conjunto estandarizado de servicios e interfaces para habilitar las funciones V2V y V2I. Proporcionan mensaje corto WAVE e IPv6 (Protocolo de Internet Versión 6) para la comunicación V2V y V2I.” [14]

2.3.6.1.7.3.8.1.8 Protocolos vehiculares

2.3.6.1.7.3.8.1.8.1 DSRC

Se basa en los estándares IEEE 1609 y IEEE 802.11p. [14]

2.3.6.1.7.3.8.1.8.2 WAVE

Protocolo de mensajes cortos. [14]

2.3.6.1.7.3.8.1.8.3 TCP / IP

Para comunicaciones V2I y V2N. [14]

2.4 Clasificación de los Riesgos 5G

El desarrollo de las Redes 5G proporciona beneficios a grande escala, pero también riesgos. “Estos se acentúan como en cualquier conexión inalámbrica, algunos son similares a las Redes cableadas, otros son nuevos.” [20]

Los usuarios no autorizados pueden obtener acceso al sistema y la información, corromper los datos, consumir Ancho de Banda de la Red, degradar el rendimiento de la Red, lanzar ataques que impiden que los usuarios autorizados accedan a los servicios o utilizar los recursos para realizar ataques en otras Redes. [8] Son múltiples riesgos en varias áreas 5G, pero se clasifican en dos tipos:

- Los ataques Pasivos y
- Los ataques Activos.

“En los ataques pasivos, los atacantes intentan aprender o hacer uso de la información de los usuarios legítimos, pero no tienen intención de atacar la comunicación en sí. Los ataques pasivos populares en una Red Celular son de dos tipos, es decir, las escuchas clandestinas y análisis de tráfico. Los ataques pasivos tienen como objetivo violar la confidencialidad de los datos y la privacidad del usuario.” [31]

“Los ataques activos en cambio, pueden implicar la modificación de los datos o la interrupción de comunicaciones legítimos. Los ataques activos típicos incluyen ataque de Hombre en el Medio (MiTM), ataque de repetición, de Denegación de Servicio (DoS) y ataque de Denegación de Servicio Distribuido (DDoS).” [31]

Según 3GPP, la transición a Redes 5G se divide en dos partes:

5G No autónomo, que depende de 4G LTE, utilizando sus mismos protocolos del Plano de Control y

5G Autónomo, donde se introduce una Red de Núcleo 5G (5GC). [30] de manera individual sin depender de LTE.

En este documento se enfoca solamente en 5G autónomo, pero la Red 5G no autónomo también se hace mención para realizar una comparativa de sus riesgos.

2.4.1 Riesgos de 5G No Autónomo

5G no autónomo se basa en protocolos de Plano de Control LTE, [30] es decir 5G híbrido, trae consigo los mismos riesgos heredados que tiene 4G, [39] inclusive otras generaciones anteriores a nivel general, simplemente por tener los mismos componentes y utilizarse de manera inalámbrica.

Las principales amenazas son:

Tabla 40 Amenazas 5G No Autónomo. Fuente: Elaboración propia basado en [30]

Amenazas NSA	Descripción
Ataque de degradación	Obliga una conexión UE LTE al conectarse a 2G o 3G. [30]
Ataque de modificación de datos	UTMS y la integridad de las comunicaciones LTE no están protegidos por el método de Seguridad para interceptar el flujo de información, esto podría dar lugar a la modificación de datos como Man in the Middle (MitM). [30]
Seguimiento de IMSI	Cuando se envían solicitudes al IMSI sin cifrar por la Radio, permite al atacante averiguar la información de la Tarjeta SIM del usuario. [30]
Roaming LTE	El uso de protocolos de señalización antiguos con vulnerabilidades antiguas. Como rastreo de mensajes, escucha de conversaciones de voz, etc.

2.4.2 Riesgos de 5G Autónomo

5G ya no depende de 4G, por lo tanto sus riesgos son independientes de 4G.

“La diferencia entre los dos tipos de 5G es la mejora de la privacidad a través de una arquitectura basada en servicios con técnicas como SDN y NFV. La Gestión Centralizada de SDN y la Virtualización de Funciones de NFV exponen las debilidades de 5G.” [30]

Algunas vulnerabilidades se deben a la arquitectura que utiliza, una autenticación débil, falta de cifrado o simplemente inseguridad en dispositivos finales. [30]

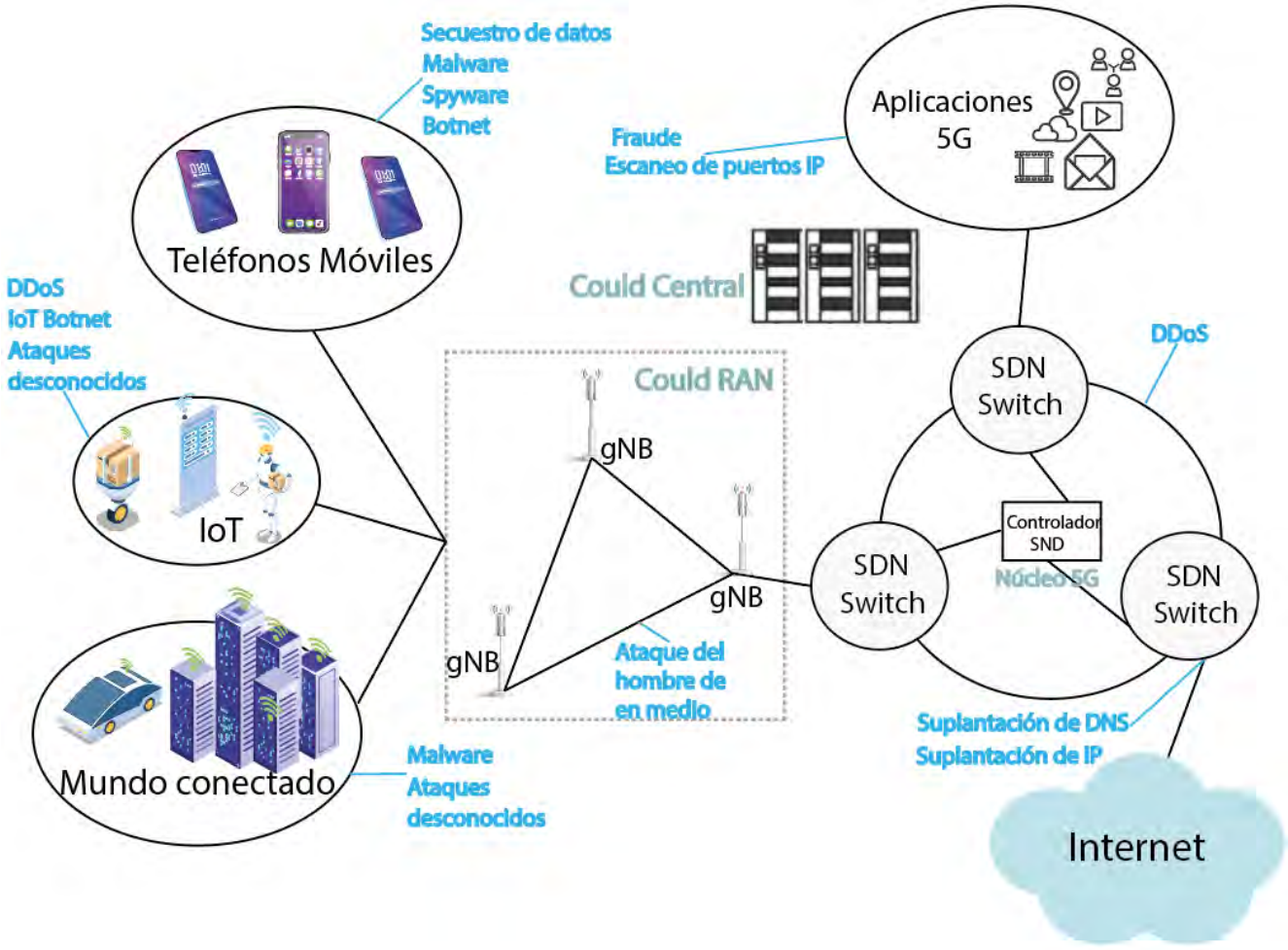


Figura 61 Ejemplos de amenazas en una Red 5G. Fuente: Ulrick Trick (2021) [19]

“El vector de amenazas 5G no tendrá fronteras y abarcará desde el equipo del usuario final como Teléfonos Móviles, artículos industriales, sensores, domótica, etc. Con un panorama de amenazas tan amplio, se extenderá en los dispositivos IoT de los usuarios finales hasta RAN e Internet.” [20]

“(Véase la Figura 61,) el posicionamiento de varios tipos de amenazas dentro de la Red, como algunos tipos de amenazas para Telefonía Móvil, incluido el Malware de Software espía, Bots, Ransomware. Se podría lanzar un MITM en el dominio de Cloud RAN, mientras que DDOs a la CN IP.” [20]

2.4.2.1 Características de las Amenazas 5G

2.4.2.1.1 Sofisticado

"De naturaleza compleja, utiliza una combinación de varias etapas de varios vectores y herramientas de ataque. Por ejemplo, el Kit de exploración Angler que está empaquetado para explotar a varios proveedores en un solo ataque." [20]

2.4.2.1.2 Ofuscatorio

"Ataques que están ocultos por múltiples Capas, difíciles de detectar." [20]

2.4.2.1.3 Evasivo

"Difícil de detectar y capacidad de ocultarse, por ejemplo ataque de Ramsomware Cryptowall y." [20]

2.4.2.1.4 Persistente

"Consistentes, evolucionan después de cada intento fallido." [20]

2.4.2.2 Amenazas

2.4.2.2.1 Amenazas de 5G Autónomo

Tabla 41 Amenazas 5G autónomo. Fuente: Elaboración propia basado en [30][31]

Amenazas SA	Descripción	Tipo de Ataque	Severidad del impacto (Extremo, Grave,

			Moderado, Menor) (1-4)
UE	Dispositivos vulnerables implica ataques de DDoS mediante solicitudes masivos al servidor para denegar el Acceso a los Recursos de la Red y ataques de Integridad de los datos almacenados en los dispositivos. [30]	Activo	Extremo
Ataque de Hombre en el Medio (MitM)	MiTM aprovecha la vulnerabilidad de dispositivos lanzando tres tipos de ataques: [30] • Ataques de Identificación, descubrimiento de dispositivos en la Red, conociendo sus características y aplicaciones. [30] • Capturar las capacidades de los dispositivos y degradar la velocidad de los datos y [30] • Ataques de agotamiento de batería. [30]	Activo	Grave
SDN y NFV	SDN mejora la flexibilidad de la Red, facilitando su gestión [43] “separando el Control de la Red del Hardware de reenvío centralizando el Control de la Red en plataformas de Controlador basados en Software acelerando la novedad de desarrollo, mejora y rápida implementación de funciones de Red.” [20] Pero los hackers pueden incrustar código en las aplicaciones del controlador SDN para restringir el Ancho de Banda en las aplicaciones del controlador de SDN y afectar negativamente las operaciones.” [43] Aplicaciones de Control	Activo	Grave

	Pueden interactuar maliciosamente tratando de ganar control sobre interruptores y controladores. [30]		
Amenazas RAN	Privacidad de los suscriptores.	Pasivo	Grave

2.4.2.2.2 Amenazas según CISA

Tabla 42 Amenazas 5G. Fuente: CISA (2021) [26] [39]

Amenaza	Descripción	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Políticas y estándares	"Los organismos de estándares pueden desarrollar controles opcionales, que no son implementados por los operadores. Al no implementar estas medidas de Seguridad subjetivas, los operadores podrían introducir brechas en la red y abrir la puerta a los actores de amenazas malintencionados." [43]	Extremo
Cadena de suministro	El uso de componentes fabricados por terceros podría exponer las entidades. Riesgos introducidos por Software y Hardware maliciosos, componentes falsificados, defectos de componentes causados por deficientes procesos de fabricación y mantenimiento. [26]	Extremo
Arquitectura	La transferencia de información en 5G se basa en Software. Esta información es sensible y confidencial. [30]	Extremo

	“La mayor densidad de componentes en la arquitectura de Red 5G.” [43]	
Seguridad en la Red	“A pesar de la mejora de la Seguridad en las generaciones anteriores, se desconoce las nuevas vulnerabilidades de 5G.“ [26]	Extremo
Competencia y elección	A pesar del desarrollo de estándares que fomentan la interoperabilidad, algunas empresas están creando interfaces patentadas en sus tecnologías, lo que limita las opciones de los clientes para utilizar otros equipos. La falta de interoperabilidad con otras tecnologías y servicios limita la capacidad de las empresas de TIC de confianza para competir en el mercado 5G. [26]	Menor

2.4.2.2.3 Sub - Amenazas según CISA

2.4.2.2.3.1 Sub - Amenazas de Políticas y estándares, según CISA

Tabla 43 Sub - Amenazas de Políticas y Estándares, según CISA 5G. Fuente: CISA (2021) [43]

Amenaza	Descripción	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Controles opcionales	Los controles de Seguridad pueden tener Redes más vulnerables y estar en mayor riesgo de ataques Cibernéticos. [43]	Grave

Estándares abiertos	Las tecnologías que no cumplen con los estándares pueden ser difíciles de reparar, actualizar, reemplazar o podrían ser completamente invisibles para el cliente. [43]	Menor

2.4.2.2.3.2 Sub - Amenazas de la Cadena de Suministro, según CISA

Tabla 44 Sub – Amenazas de Cadena de Suministro, según CISA 5G. Fuente: CISA (2021) [43]

Amenaza	Descripción	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Componentes falsificados	"Son más susceptibles a los Ciberataques y es más probable que se rompan, por su mala calidad. Los componentes falsificados comprometidos podrían habilitar un actor para afectar la confidencialidad, integridad o disponibilidad que viajan a través de dispositivos y moverse lateralmente a otras partes más sensibles de la Red." [43]	Moderado

Componentes heredados	“Pueden provenir de cadenas de suministro extendidas que consisten en proveedores externos, vendedores y proveedores de los servicios.” [43] “Estas pueden verse comprometidos a través de ataques a proveedores, incluidos los proveedores de proveedores, que pueden tener controles de Seguridad y auditorías más débiles en sus canales de desarrollo, producción o distribución. Defectos de Malware insertados.” [43]	Moderado

2.4.2.2.3.3 Sub - Amenazas de Arquitectura de Sistemas 5G, según CISA

Tabla 45 Sub – Amenazas de Arquitectura de Sistemas 5G, según CISA 5G. Fuente: CISA (2021) [43]

Amenaza	Descripción	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Seguridad en la Red	“Las nuevas capacidades de Infraestructura como torres Celulares, Formación de Haces, Celdas pequeñas y dispositivos Móviles, presentan una oportunidad para que los actores malintencionados expongan vulnerabilidades a través de un mayor conjunto de vectores de amenazas.” [43]	Extremo
Configuración de Software	“El acceso no autorizado a Software o componentes de Red proporciona a un actor malintencionado la	Grave

	oportunidad de modificar configuraciones para reducir los controles de Seguridad, instalar Malware en el sistema o identificar las debilidades en el producto.” [43]	
Segmentación de la Red	“La administración inadecuada de segmentos de Red puede permitir que los actores malintencionados accedan a los datos de diferentes sectores o denegar el Acceso a los usuarios priorizados.” [43]	Grave
Compartir espectro	Para los diferentes casos de uso para la utilización 5G, se requiere los tres tipos de Frecuencias, baja, media y alta. Con el aumento del número de dispositivos que compiten con el espectro que muchas veces se encuentran agotado, es necesario compartir espectro. [43] “El uso compartido del espectro puede brindar a los hackers de sombrero negro oportunidades para interferir con rutas de comunicación no críticas, lo que afecta negativamente las Redes de comunicaciones más críticas.” [43]	Moderado

2.4.2.2.3.4 Sub - Amenazas de SDN

Tabla 46 Desafíos de Seguridad de SDN. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) [20][31]

Capa SDN	Vulnerabilidades	Descripción de Riesgos	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)

Solicitud	Falta de Autenticación y Autorización Reglas fraudulentas Falta de Control de Acceso y responsabilidad	No existen mecanismos convincentes para la autenticación y autorización de aplicaciones, y es más amenazante en el caso de gran cantidad de aplicaciones de terceros. Las aplicaciones maliciosas pueden generar reglas de flujo falsas. Un problema para el plano de la gestión y el uso ilegal de los recursos de la Red.	Extremo
Control	DoS, Ataque DDoS Acceso al controlador no autorizado Escalabilidad o Disponibilidad	Debido a la naturaleza visible del Plano de Control. No hay mecanismos convincentes para obligar el control de acceso a las aplicaciones. Es muy probable que la centralización de la Inteligencia en una entidad presente desafíos de Escalabilidad y Disponibilidad.	Extremo

Plano de datos	Reglas de flujo fraudulentas. Ataques por inundaciones Secuestro del controlador	El Plano de Control es susceptible a reglas de flujo fraudulentas. Las Tablas de flujo de los interruptores de OpenFlow pueden almacenar un número infinito o limitado de Reglas de Flujo. En el Plano de Datos depende del Plano de Control, por lo que su Seguridad depende de la Seguridad del controlador.	Grave
Control de Datos	Ataques de nivel TCP	TLA es vulnerable a los ataques a nivel TCP.	Grave

2.4.2.2.4 Ataques en Redes Inalámbricas, según Rose Fang, Yi Qian

Tabla 47 Ataques en Redes Inalámbricas según Dongfeng Fang, Rose QingyangHu, Yi Qian (2018) [31]

Amenazas	Descripción	Tipo de Ataque	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Interferencias	Interferencias intencionales para irrumpir comunicaciones. [31]	Activo	Grave
Escuchas clandestinas	Escuchar a escondidas permite una comunicación normal sin ningún tipo de	Pasivo	Moderado

	intervención, haciéndolo difícil de detectar. [31]		
Análisis de tráfico	Interceptación de la Información. [31]	Pasivo	Moderado

2.4.3 Clasificación de los Riesgos IoT

2.4.3.1 Amenazas generales IoT

Tabla 48 Amenazas generales IoT. Fuente: Elaboración propia basado en [8][19][31]

Amenazas Generales IoT	Tipo de Ataque	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Puertos seriales expuestos.		Extremo
Mecanismos de Autenticación inseguro utilizado en los puertos serie.	Activo	Extremo
Ataques basados en medios extremos.	Activo	Extremo
Ataques de DDoS.	Activo	Extremo
Posibilidad de volcar el Firmware a través de JTAG, o mediante Chips Flash.	Activo	Grave

2.4.3.2 Vulnerabilidades de los componentes IoT

Tabla 49 Vulnerabilidades de los componentes IoT. Fuente: Elaboración propia basado en [8][31]

Componente IoT	Vulnerabilidades	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
	Verificaciones de Autenticación y autorización inseguras.	Extremo

Aplicaciones Móviles	Fuga de datos del canal general. Ataques de manipulación en tiempo de ejecución. Ingeniería Inversa de la Aplicación Móvil. Comunicación de Red Inseguras. Defectos empresariales y lógicos.	Grave. Grave Grave Moderado Menor
Panel de Control basado en Web	Autenticación y autorización inseguras. Fuga de datos sensibles. Falsificación de solicitudes entre sitios. Secuencias de comandos entre sitios. Inserción del lado del cliente. Referencia del objeto directo inseguro.	Extremo Extremo Grave Grave Grave Menor
Firmware	Valores confidenciales codificados por Firmware, contraseñas y URL de ensayo. Capacidad de comprender toda la funcionalidad del dispositivo a través del Firmware. Extracción del sistema de archivos del Firmware. Componentes obsoletos con vulnerabilidades conocidas. Posibilidad de modificar el Firmware. Verificación de la Integridad y firma insegura.	Extremo Extremo Extremo Grave Grave Grave

2.4.3.3 Vulnerabilidades en los Protocolos y medios de comunicación de Radio IoT

Tabla 50 Amenazas en los protocolos y medios de comunicación de Radio. Fuente: Elaboración propia basado en [8]b[31]

Amenazas en los Protocolos y medios de comunicación de Radio	Tipo de Ataque	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Ataques de intermediario.	Activo	Extremo
Ataques basados en repetición.	Activo	Extremo
Denegación de Servicio.	Activo	Extremo
Falta de cifrado (DDoS).		Extremo
Capacidad para extraer información sensible de paquetes de Radio.		Extremo
Interceptación y modificación de comunicaciones de Radio en Vivo.	Activo	Extremo
Verificación de la redundancia cíclica insegura (CRC).		Grave

2.4.3.4 Amenazas en Vehículos Autónomos

Tabla 51 Amenazas en Vehículos Autónomos. Fuente: Elaboración propia basado en [31][41]

Amenazas en los Vehículos Autónomos		Tipo de Ataque	Severidad del impacto (Extremo, Grave, Moderado, Menor) (1-4)
Amenazas a la Confidencialidad	Inspección de mensajes V2P y dirigir peatones a situaciones peligrosas.	Activo	Extremo

	Inspección de mensajes V2V y V2I de las RSU.	Pasivo	Extremo
	Fuga de Información de Identificación Personal.	Pasivo	Extremo
	Inspección de mensajes V2V entre una Unidad de Central de Comunicación y un dispositivo nómada.	Pasivo	Grave
Amenazas a la Integridad	Manipulación de Información de Sensores.	Activo	Extremo
	Desbordamiento de Buffer Vehicular.	Activo	Extremo
	Ataque de denegación de Servicio Vehicular.	Activo	Extremo
	Manipulación de mensajes de encaminamiento.	Activo	Grave
	Manipulación de Información de Credenciales.	Activo	Moderado
Amenazas a la Disponibilidad	Desbordamiento de Buffer Vehicular.	Activo	Extremo
	Ataque de Denegación de Servicio Vehicular.	Activo	Extremo
	Ataque de temporización.	Activo	Moderado
	Hack de sensores.	Activo	Menor
Amenazas a la Autenticidad	Ataque de modificación de LMD y la Tabla de Encaminamiento.	Activo	Grave
	Ataque de suplantación.	Activo	Moderado

	Ataque de Sibila.	Activo	Moderado
	Manipulación de la Base de Datos de Certificación.	Activo	Moderado
Amenazas a la Imputabilidad	Duplicación no autorizada de un dispositivo nómada.	Activo	Grave
	Duplicación no autorizada de un vehículo y una RSU.	Activo	Grave
Amenazas a la Autorización	Acceso no autorizado a la información de Seguridad de un vehículo.	Activo	Grave

2.4.3.5 Otras Amenazas

Tabla 52 Otras Amenazas. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) [20][31]

Amenazas	Descripción	Tipo de Ataque	Severidad del impacto (Menor, Moderado, Grave, Extremo) (1-4)
Mimo Masivo	El número de antenas MIMO Masivo.	Activo	Extremo
Malware avanzado	“Malwares avanzados dirigidos a miles de millones de dispositivos móviles e IoT extremos con capacidad de explotar el Sistema Operativo y las Vulnerabilidades de la Red.” [20]	Activo	Extremo
Secuestro de datos	“Los malwares especializados explotan, cifran, bloquean el acceso a los datos críticos, para poder conceder el acceso	Activo	Grave

	después de un pago de rescate exigido.” [20]		
Riesgos críticos de infraestructura	“Amenazas enfocadas que dañan servicios de infraestructura crítica como SCADA, es decir, Stuxnet, ataques de Shamoon.” [20]	Activo	Extremo
Ataques de día cero	Un ataque avanzado que aprovecha las vulnerabilidades no descubiertas de un sistema. Puede ser una combinación o paquete de múltiples tipos de ataques, malware, rootskits y botnets. [20]	Activo	Extremo
Botnet’s IoT y Botnet’s Móviles	“IoT y dispositivos móviles que alojan un agente / bot de control que recibe comandos remotos y filtra continuamente información telemetría a un bot maestro remoto que ejecuta un sistema central de comando y control (C%C). Se utiliza tanto para ataques pasivos como activos.” [20] “Los Botnets móviles son ideales para el Control Remoto de Máquinas.” [37]	Activo / Pasivo	Grave

2.5 Análisis de los Riesgos 5G

Véase páginas 4 – 6, 11 del Capítulo 1.

2.5.1 Descripción

Dados los Riesgos identificados que amenazan la Seguridad de las Redes 5G, los usuarios, organizaciones, intereses nacionales, clasificados por tipo de división de transición a Redes 5G autónomo y no autónomo, autor, tipo de ataque pasivo o activo. [43]

Según Cisco, los ataques de Red son clasificados por Reconocimiento, Acceso y Denegación de Servicio. [1]

2.5.1.1 Tipos de Ataques a la Red, según Cisco

2.5.1.1.1 Ataques de Reconocimiento

"Es la detección y esquematización no autorizadas de Sistemas, servicios o vulnerabilidades." [34]

2.5.1.1.1.1 Ejemplos de ataques de Reconocimiento

2.5.1.1.1.1.1 Arquitecturas de Red 5G

- Gestión inadecuada de las entidades y accesos debido a la escalabilidad insuficiente. [19]
- Interfaces y API inseguras para la administración, gestión, orquestación y acceso a usuarios. [19]
- Debilidades en el Software del Sistema y la aplicación debido a errores. [19]
- Asumir cuentas de los usuarios al robar su información de inicio de sesión como resultado de phishing, fraude o explotación de errores. [19]

- Personas internas malintencionadas, empleados actuales o interiores del operador de infraestructura de nube.
- Amenazas persistentes avanzadas (APT).
- Perdida de datos debido a la eliminación involuntaria, incendio, daños por agua o desastres naturales. [19]
- Uso indebido de servicios de la nube. [19]
- Compartir recursos. [19]
- Seguridad insuficiente de la infraestructura física. [19]

2.5.1.1.1.1.2 Seguridad en la Red

"A pesar de la mejora de la Seguridad en las generaciones anteriores, se desconoce las nuevas vulnerabilidades de 5G." [26]

"Los fabricantes de los componentes y los proveedores de servicios están desarrollando tecnologías y especificaciones de Seguridad para mitigar las vulnerabilidades en las Redes Inalámbricas." [26] "5G llevará los componentes de las TIC y la Gestión de Datos al límite de la Red, lo que mejorará la Seguridad a través de la Segmentación de la Red, Funciones de Autenticación, y detención o las respuestas automatizadas frente a amenazas. Implementados correctamente, limita la capacidad de los atacantes para acceder a la Red, la migración de funciones de Red aumentará la potencia de Gestión de la Red." [26]

Aun así, con nuevas mejoras de Seguridad 5G, se desconoce las vulnerabilidades reales que podría tener la nueva Red, es probable que los Protocolos o inclusive los equipos ya sea por los componentes de diferentes proveedores, tenga vulnerabilidades desconociendo el origen de estas, por lo tanto, cualquier vulnerabilidad inherente a 5G, las tecnologías pueden ser explotadas de cualquier manera, aún que ya se hayan desarrollado las correcciones, porque los atacantes siempre están en constante evolución. *Véase página 5.*

2.5.1.1.1.1.3 SDN

2.5.1.1.1.1.3.1 Plano de datos

- Pueden manipular las tablas de flujo accediendo a una o más conmutaciones. [19]
- SDN. Pueden modificar paquetes de datos, omitir funciones de Red de Seguridad, o reenviar paquetes a objetivos definidos por ellos. Inundación de paquetes de flujos previamente desconocidos puede afectar el rendimiento de la Red SDN. [19]

2.5.1.1.1.1.3.2 Plano de Control

- Acceso no autorizado al Plano de Control, fácil manipulación del tráfico total de datos a través de la posible configuración de los conmutadores SND y las tablas de Flujo. Esto no solo puede afectar a los usuarios finales, sino también la gestión y la orquestación de la Red. [19]
- La funcionalidad del controlador debe estar protegida por redundancia, control de acceso, Software contra virus y gusanos, Firewall, detección de intrusiones y sistemas de prevención de intrusiones. [19]

2.5.1.1.1.1.3.3 SBI

- Interfaz en riesgo por toma de control, dando un efecto dañino, los interruptores SDN pueden manipularse. [19]

NFV, controles opcionales, componentes falsificados, componentes heredados.

2.5.1.1.2 Ataques de Acceso

"Manipulación no autorizada de datos, de accesos al sistema o de privilegios de usuario." [34]

Se realiza el enfoque de prueba y error para adivinar contraseñas por ejemplo infinidad de intentos para adivinar nombres de usuario y contraseña en grandes masas, se hace uso de herramientas que de manera automática, permite probar infinidad de combinaciones en el mejor tiempo posible (ataque de fuerza bruta). Después que el atacante gana el acceso al recurso, tiene los mismos derechos de acceso del usuario. [1]

Existen 5 tipos de Ataques de Acceso:

2.5.1.1.2.1 Ataque de Contraseña

Es una forma de obtener contraseñas a fuerza bruta utilizando herramientas especializadas. Los ataques de fuerza bruta se realizan simultáneamente con ayuda de un diccionario. El Diccionario se conforma por múltiples contraseñas y usuarios posibles de manera aleatoria. [1]

2.5.1.1.2.2 Cambio de Dirección del Puerto

El número de puertos se usa para la comunicación de extremo a extremo si se envía un mensaje este se identifica y contiene información hacia dónde se dirige. Dependiendo del servicio que se requiere es el número de puerto. [1]

Por lo tanto, un cambio de dirección de puerto provoca la pérdida del mensaje para el receptor. [1]

2.5.1.1.2.3 Hombre en el Medio

En una comunicación de extremo a extremo el atacante se posiciona en el medio para espiar, modificar la información, copiar todo el tráfico transmitido, hacerse pasar por el receptor y el transmisor al mismo tiempo. Al detectar una cantidad inusual de actividades de la Red y el uso excesivo del Ancho de Banda se puede determinar existe en la Red un Hombre en el Medio. [1]

MITM tiene como objetivo comprometer la Confidencialidad, Integridad y Disponibilidad de los Datos. [31]

2.5.1.1.2.3.1 Cadena de Suministro

“Con el potencial para la conexión de miles de millones de dispositivos 5G, existe un mayor riesgo de componentes no confiables o falsificados que se introducirán en la cadena de suministro 5G. Esto podría incluir dispositivos o infraestructura comprometidos que

finalmente afecten a los dispositivos del usuario final, como computadoras, teléfonos y otros dispositivos. Empresas que no son de confianza o proveedores respaldados por el gobierno, también contribuyen al riesgo de la cadena de suministro, especialmente aquellos que tienen importantes cuotas de mercado dentro de las Redes de Telecomunicaciones.

Por ejemplo, aquellos países que compran los equipos 5G de empresas con cadenas de suministro comprometidas podrían ser vulnerables a interceptación, manipulación, interrupción o destrucción de datos.

Esto plantearía un desafío al enviar datos a socios internacionales, donde la Red segura de un país podría ser vulnerable a amenazas debido a una Red de Telecomunicaciones que no es de confianza en otro país.” [26] [43]

Por ejemplo, pueden afectar el rendimiento de la Red y comprometer la Confidencialidad, Integridad y Disponibilidad de los activos de la Red. [26]

2.5.1.1.2.3.2 Escuchas Clandestinas

“Es un ataque que utiliza un receptor no intencionado para interceptar un mensaje de otros.” [31]

2.5.1.1.2.3.3 Análisis de Tráfico

Se utiliza para interceptar información como la ubicación y la identidad de las partes de la comunicación mediante el análisis del tráfico de la señal recibida sin comprender el contenido de la señal en sí. [31]

2.5.1.1.2.3.4 Interferencias

“Pueden irrumpir por completo las comunicaciones entre usuarios legítimos. Un nodo malicioso puede generar interferencias intencionales que pueden interrumpir las comunicaciones de datos entre usuarios legítimos. La interferencia también puede evitar que los usuarios autorizados accedan a los recursos de Radio.” [31]

2.5.1.1.2.3.5 Helnet

Es un sistema conformado por niveles, con diferentes características cada una, por ejemplo, la potencia de transmisión, el tamaño de cobertura o el Acceso Radio, Con estas características, se logra una cobertura más amplia y mayor capacidad de rendimiento. [31]

En comparación con una Red Celular de un solo nivel, los equipos de usuario son más vulnerables a escuchas clandestinas. Además, la densidad de Celdas pequeñas en Helnet, los mecanismos de traspasos tradicionales podrían enfrentar importantes problemas de rendimiento debido a traspasos demasiado frecuentes entre diferentes Celdas. [31]

La alta densidad de Celdas pequeñas permite la facilidad de revelar la información de ubicación del usuario debido al conocimiento de la Celda con la que está asociado un usuario. [31]

2.5.1.1.2.3.5.1 Privacidad Helnet

"La información de ubicación se vuelve más vulnerable a la alta densidad de Celdas pequeñas." [31] el algoritmo de asociación puede revelar la privacidad de la ubicación de los usuarios. [31]

Segmentación de la Red, compartir espectro.

2.5.1.1.2.4 Desbordamiento de Buffer

Para almacenar datos de entrada de manera temporal como zona de memoria se utiliza el buffer saturar este servicio causa bloqueo que la aplicación y no se puede ejecutar de manera correcta. [1]

2.5.1.1.2.5 Explotación de Confianza

El atacante de manera no autorizada compromete el sistema utilizando privilegios de los usuarios después de realizar un ataque de contraseña. [1]

2.5.1.1.3 Ataque de Denegación de Servicio

"Consisten en desactivar o dañar redes, Sistemas o servicios." [34]

Existen diferentes maneras, pero la más común es provechar una o varias vulnerabilidades para consumir recursos, con el propósito de saturar la Red con tráfico basura, sin que pueda realizar la traducción de URL en direcciones IP, dejando inutilizables servicios que se proporcionan a los usuarios. [1]

2.5.2 Análisis de los Riesgos IoT

Examine páginas 6 – 11 con el tema de: "Ciber" y los tipos de Ciberataques generales.

2.5.2.1 Antecedentes de Riesgos IoT

Los responsables en la formulación de las políticas IoT, trataron de competir con el aumento de dispositivos IoT, pero debido a su incremento repentino, no pudieron establecer controles de calidad muy estrictos y regulaciones de Seguridad. [8]

A pesar de adoptar un número significativo de dispositivos IoT, ignoraron las consideraciones de Seguridad.

Fue hasta que Botnet Mirai, demostró las deficiencias de Seguridad de los dispositivos IoT al atacarlos, en su mayoría cámaras conectadas a Internet. [8]

"En los últimos años, aunque la Seguridad de estos dispositivos ha mejorado lentamente, aún no ha llegado a un punto en el que estos dispositivos puedan considerarse extremadamente seguros para usar. Se ha determinado que todos los dispositivos inteligentes tienen problemas críticos de Seguridad y privacidad, incluidos los Sistemas Inteligentes de automatización del hogar, dispositivos portátiles o monitoreo para bebés." [8]

2.5.2.1.1 Problemas anteriores de IoT

2.5.2.1.1.1 El hack Jeep

"Los investigadores Dr. Charlie Miller y Chris Valasek demostraron en el 2015 como podían hacerse cargo y controlar de manera remota un Jepp utilizando las vulnerabilidades

en el Sistema Uconnect de Chrysler, lo que provocó que esa empresa tuviera que retirar 1,4 millones de vehículos. [8]

Esto aprovechó muchas vulnerabilidades diferentes incluidos los esfuerzos de la Ingeniería Inversa aplicada en varios protocolos individuales. La vulnerabilidad del Software Uconnect permitió conectarse de manera remota a través de una conexión Celular, accediendo al puerto 6667 con una autenticación anónima habilitada, encontrando que ejecutaba D-Bus sobre IP, forma de comunicación entre procesos. De igual manera tenía un método de ejecución que permitía a los investigadores ejecutar código arbitrario en el dispositivo (ver Figura 62).” [8]

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/ha
rman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.Ser
viceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 |
/bin/sh | netcat 192.168.5.109 6666"}')
```

Figura 62 Explotar código. Fuente: Aditya Gupta (2019) [8]

2.5.2.1.1.2 Belkin Wemo

“Belkin Wemo es una línea de productos que ofrece a los consumidores la automatización de toda la casa.” [8]

Este caso es relevante en la historia de IoT porque provocó la instalación de Firmware malicioso en el dispositivo. Al momento de realizar actualizaciones a través de un canal no cifrado, permitió que los atacantes modificar el paquete binario de Firmware durante la actualización. Al darse cuenta del riesgo que se estaba produciendo, se utilizó un mecanismo de distribución de Firmware cifrado basado en GNU Privacy Guard (GPG) para que el dispositivo no aceptara paquetes de Firmware maliciosos inyectados por un atacante. [8]

2.5.2.1.1.3 Bomba de insulina

“Un investigador de Seguridad llamado Jay Radcliffe que trabajaba para Rapid7 identificó que algunos dispositivos médicos, especialmente las bombas de insulina podrían estar sufriendo una vulnerabilidad de ataque basada en la repetición, Radcliffe, un diabético

tipo 1, se propuso a investigar una de las bombas de insulina más populares del mercado, el sistema de bomba de insulina OneTouch Ping de Animas, una subsidiaria de Johnson & Johnson. Durante el análisis, descubrió que la bomba de insulina enviaba mensajes de texto sin cifrar para comunicarse, lo que hacía que fuera extremadamente sencillo para cualquiera capturar la información, modificar la dosis de insulina que administraría y retransmitir el paquete. Cuando probó el ataque a la bomba de insulina, funcionó a la perfección, sin que hubiera forma de saber la cantidad de insulina que se administraba durante el ataque.

La vulnerabilidad fue parcheada por el proveedor, de al menos 5 meses, lo que demuestra que al menos algunas empresas se toman en serio los informes de Seguridad y toman medidas para mantener seguros a los consumidores.” [8]

2.5.2.1.1.4 Hackear armas y rifles inteligentes

Además de los típicos dispositivos y electrodomésticos inteligentes que comúnmente suelen relacionarse dentro de IoT como casas o ciudades inteligentes, los rifles también entran dentro del grupo. “TrackingPoint, uno de los fabricantes de tecnología de rifle inteligente, ofrece una aplicación móvil para mirar la vista de disparo y ajustarla. Se descubrió que esta aplicación es vulnerable a un par de problemas de Seguridad. Runa Sandvik y Michael Auger identificaron las vulnerabilidades en el rifle inteligente que les permitía acceder a las interfaces de programación de aplicaciones (API) de administración después de obtener acceso al dispositivo a través de UART. Al explotar la aplicación Móvil, un atacante basado en la Red permitiría a un atacante cambiar los diversos parámetros, como la velocidad del viento y la dirección el peso del viento.” [8] Al modificarse esos parámetros, el tirador no sabe que se han realizado cambios, porque es un riesgo para la integridad física de las personas. [8]

Estos ejemplos de vulnerabilidades, según Aditya Gupta (2019) ayuda a comprender varios tipos de vulnerabilidades que normalmente se encuentran en los dispositivos IoT. [8]

2.5.2.1.2 Razones de las vulnerabilidades de Seguridad IoT

Como se ha mencionado al inicio del tema “Clasificación de riesgos IoT”, de a acuerdo al incremento de IoT, no se ha podido controlar la calidad de manera estricta y a veces las

regulaciones de Seguridad son casi nulas o cuentan con un sistema complejo, a su vez las causas de problemas de Seguridad al construir estos dispositivos se dan a continuación: [8]

2.5.2.1.2.1 Falta de conciencia de Seguridad entre los desarrolladores

La mayoría de los desarrolladores IoT desconocen las posibles vulnerabilidades de Seguridad en los dispositivos IoT. [8]

2.5.2.1.2.2 Falta de una perspectiva macro

Falta de análisis de los posibles riesgos que se pudieran dar en la arquitectura completa del dispositivo, realizando un modelado de amenazas. [8]

2.5.2.1.2.3 Problemas de Seguridad basados en la cadena de suministro

Diferentes componentes son fabricados por diferentes proveedores, ensamblado por otro proveedor, y distribuido por alguien diferente a los primeros proveedores, genera problemas de Seguridad (puerta trasera) poniendo en riesgo el producto. [8]

2.5.2.1.2.4 Uso de marcos inseguros y bibliotecas de terceros

El uso de bibliotecas y paquetes existentes o la inserción de muestras de código potencialmente vulnerables en el producto seguro. [8]

2.5.2.2 Vulnerabilidades generales IoT

Las siguientes son las vulnerabilidades encontradas en los dispositivos:

Tabla 53 Vulnerabilidades IoT. Fuente: [8][19]

Vulnerabilidades generales IoT
Puertos seriales expuestos.
Mecanismo de autenticación inseguro utilizado en los puerto serie.
Posibilidad de volcar el firmware a través de JTAG, o mediante chips Flash.
Ataques basados en medios extremos.
Ataques de DDoS.

2.5.2.3 Vulnerabilidades en los componentes IoT

Examine tema: "Componentes IoT" en las páginas 128 – 129.

Los componentes IoT se organizan en aplicación Móvil, el Panel de Control basado en Web, las Interfaces de Red seguras y el Firmware. Estos componentes también cuentan con problemas de Seguridad y son los siguientes: [8]

Tabla 54 Vulnerabilidades de los componentes IoT. Fuente: Elaboración propia basado en [8]

2.5.2.4 Vulnerabilidades en los Protocolos y medios de comunicación de Radio

Algunos de los protocolos de comunicación por Radio comunes que se utilizan en los dispositivos IoT son celulares, Wi-Fi, BLE, ZigBee, Wave, 6LoWPAN, LoRa. [8]

Dependiendo del protocolo de comunicación que utilice el dispositivo, se podrá requerir hardware especializado para realizar el análisis de la comunicación por Radio. [8]

Tabla 55 Vulnerabilidades en los protocolos y medios de comunicación de Radio. Fuente: Elaboración propia basado en [8]

Vulnerabilidades en los protocolos y medios de comunicación de Radio
- Ataques de intermediario.
- Ataques basados en repetición.
- Verificación de la redundancia cíclica insegura (CRC)
- Ataques basados en interferencias.
- Denegación de servicio.
- (DoS) Falta de cifrado.
- Capacidad para extraer información sensible de paquetes de Radio.
- Interceptación y modificación de comunicaciones por Radio en Vivo.

2.5.2.5 Vulnerabilidades en Vehículos autónomos

Se tiene un ejemplo de caso de uso, los vehículos autónomos y sus riesgos.

2.5.2.5.1 Tipos de amenazas Vehiculares

Existen diferentes tipos de amenazas vehiculares, según el tipo de comunicación V2X. Cada figura ilustra los conceptos de cada tipo de amenaza.

2.5.2.5.1.1 Amenazas a la Confidencialidad

"Un atacante puede inspeccionar los mensajes V2V de los vehículos cercanos para leerlos o guardarlos y mensajes V2I de las RSU y analizar la información del tráfico mediante el procesamiento de los mensajes inspeccionados.

Un atacante puede inspeccionar los mensajes V2V entre una Unidad Central de Comunicación y un dispositivo nómada para, entonces, analizar la información dinámica del vehículo como su localización y velocidad.

Un atacante puede inspeccionar los mensajes V2P y dirigir intencionalmente a los peatones hacia situaciones viales peligrosas." [41]

2.5.2.5.1.1.1 Fuga de Información de Identificación Personal (IIP)

“Un atacante puede analizar la información para descubrir quién es el propietario del vehículo gracias a los mensajes V2X y rastrear la localización de una persona concreta a lo largo del camino.” [41]

(Examine la Figura 63) las diferentes amenazas de Confidencialidad descritos anteriormente.

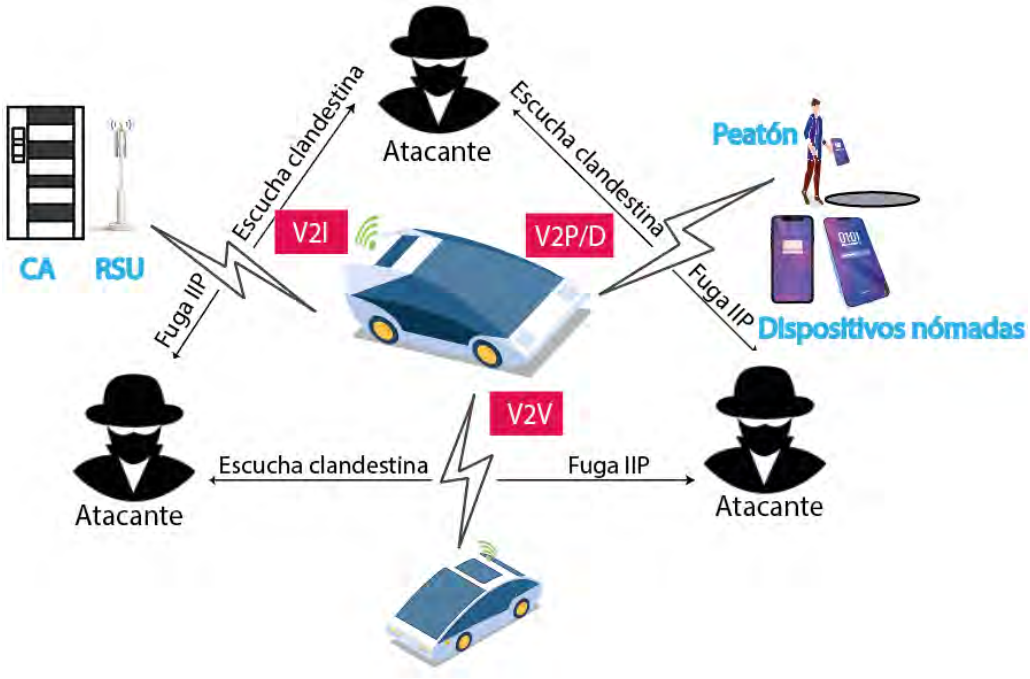


Figura 63 Amenazas de Confidencialidad. Fuente: UIT-T (2020) [41]

2.5.2.5.1.2 Amenazas a la Integridad

Las amenazas a la Integridad son las siguientes:

2.5.2.5.1.2.1 Manipulación de mensajes de encaminamiento

Un nodo intermedio maligno modifica los mensajes de encaminamiento y los vehículos reciben información falsa. [41]

2.5.2.5.1.2.2 Manipulación de Información de credenciales

“Es la modificación de la clave privada o el ID del vehículo de manera que el atacante puede utilizar la información de credenciales de otro vehículo sin autorización.” [41]

2.5.2.5.1.2.3 Manipulación de Información de sensores

Un atacante puede modificar la dirección física de un módulo de comunicación o manipular la información de la ECU, por ejemplo, el sensor de velocidad, radares o cámaras. Es posible comunicar otras OBU o RSU datos de sensores falsos, incluidos datos como la latitud, velocidad, ángulo del volante y la aceleración siendo manipulados pueden causar problemas con el tráfico. [41]

(Ver la Figura 64) las diferentes amenazas a la Integridad, descritos anteriormente.

Las aplicaciones manipuladas pueden tener efectos nocivos en los vehículos, inclusive pueden poner en riesgo la vida de diferentes números de personas a través de la Interfaz de comunicación V2D. [41]

2.5.2.5.1.2.4 Desbordamiento de Buffer Vehicular

Entre otros casos, una aplicación manipulada puede forzar a un dispositivo nómada infinidad de mensajes vacíos a la OBU, con el fin de saturar el servicio vehicular mediante la inundación de mensajes. [41]

2.5.2.5.1.2.5 Ataque de Denegación de Servicio Vehicular

Es posible de la misma un atacante de manera no autorizada mediante una aplicación manipulada transfiera código maligno a una OBU, consumiendo todos los recursos del sistema, dejando inutilizable los servicios que proporciona. [41]

Figura 64 Amenazas a la Integridad. Fuente: UIT-T (2020) [41]

2.5.2.5.1.3 Amenazas a la Disponibilidad

2.5.2.5.1.3.1 Interferencia Deliberada y Ataque de Denegación de Servicio Distribuida (DDoS)

(ver Figura 65)

2.5.2.5.1.3.1.1 Desbordamiento de Buffer

Un atacante puede enviar múltiples mensajes innecesarios o vacíos mediante la inundación de mensajes. Dentro de esa categoría de ataques se cuenta el simple reenvío de un mensaje específico mediante un nodo de encaminamiento hasta saturar el servicio causando bloqueo de la aplicación, sin que se pueda ejecutar de manera correcta. [41]

2.5.2.5.1.3.1.2 Ataque de Denegación de Servicio Vehicular

Es posible de la misma un atacante de manera no autorizada mediante una aplicación manipulada transfiera código maligno a una OBU, consumiendo todos los recursos del sistema o simplemente causando bloqueo temporal del sistema enviando múltiples mensajes cuya

capacidad supera la capacidad de almacenamiento del Buffer[58], dejando inutilizable los servicios que proporciona. [41]

2.5.2.5.1.3.1.3 Ataque de Temporización

"Un atacante de temporización consiste en retrasar la entrega de los mensajes de Seguridad de otros vehículos de modo que se impida la adecuada ejecución de los servicios de comunicación V2X, como la Radio fusión de mensajes de alerta." [41]

2.5.2.5.1.3.2 Hack de Sensores

Para causar fallos en los sensores. Existen dos tipos de fallos de sensores: los transitorios y permanentes. Los fallos transitorios permanecen en un periodo corto de tiempo y pueden darse durante un funcionamiento normal del sistema, pero desaparecen rápidamente sin necesidad de reparación, por ejemplo, cuando el GPS pierde conexión con los satélites. Los fallos permanentes, son los que persisten inclusive aún con reparación, teniendo como primer y último recurso la reposición de un nuevo sensor. Estos fallos al darse en un periodo muy extendido afectan gravemente el funcionamiento del sistema. [41]

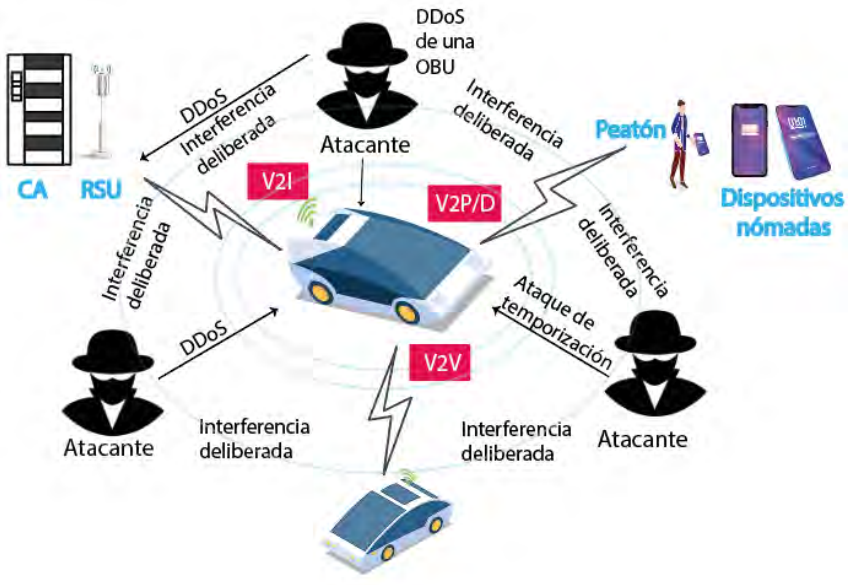


Figura 65 Amenazas a la Disponibilidad. Fuente: UIT-T (2020) [41]

[58] Almacenamiento temporal de datos.

2.5.2.5.1.4 Amenazas a la Autenticidad

2.5.2.5.1.4.1 Ataque por modificación de LMD y la Tabla de Encaminamiento

(Ver Figura 66)

"Un atacante puede falsificar la información del GPS de un vehículo y modificar su información geoespacial original." [41]

2.5.2.5.1.4.1.1 Ataque por Suplantación

"El atacante puede aparentar ser otra identidad tras haber robado la información de entidad de esa entidad, recibiendo los mensajes que normalmente se envían a la otra entidad y enviar mensajes como si también lo fuera." [41] Por ejemplo, si esa identidad fuera una patrulla de policía, el atacante podrá enviar mensajes de alerta de persecución a los demás vehículos para que le den paso.

2.5.2.5.1.4.2 Ataque de Sibila

"Un ataque de Sibila es aquel en el que, por ejemplo, un vehículo simula ser múltiples vehículos utilizando múltiples ID de vehículo.

2.5.2.5.1.4.2.1 Manipulación de la Base de Datos de Certificación

"Un atacante puede manipular la Base de Datos de pseudónimo de la CA y posteriormente modificar la relación entre un certificado a largo plazo y un certificado de seudónimo a corto plazo." [41]

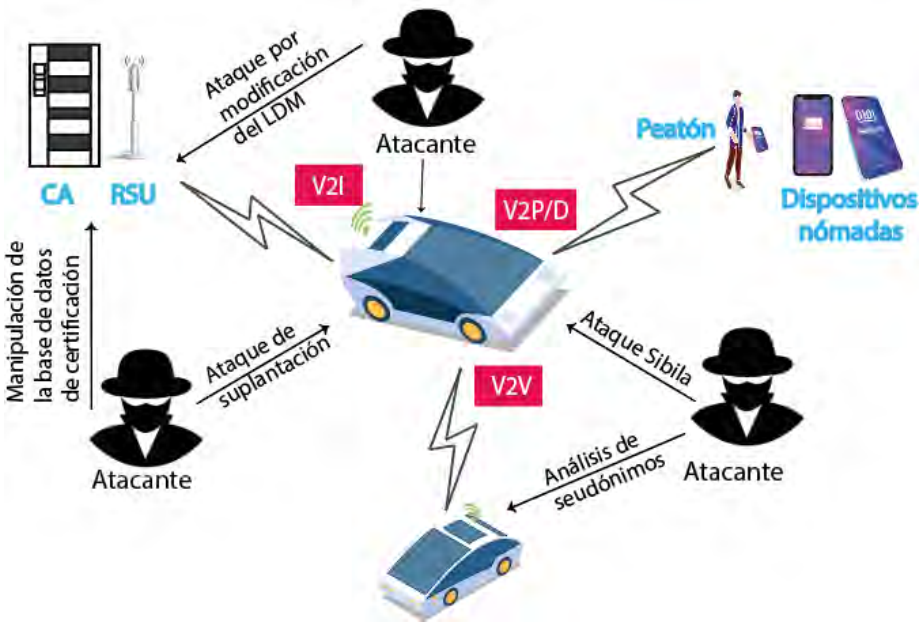


Figura 66 Amenazas a la Autenticidad. Fuente: UIT-T (2020) [41]

2.5.2.5.1.5 Amenazas a la Imputabilidad

2.5.2.5.1.5.1 Duplicación No Autorizada de un Dispositivo Nómada

2.5.2.5.1.5.1.1 Explotación de Confianza

(Ver Figura 67.) Es un tipo de ataque que se llama explotación de confianza, este se lleva a cabo cuando un atacante de manera no autorizada compromete el sistema utilizando privilegios de los usuarios después de realizar un ataque de contraseña. [1]

Por ejemplo, para algunos servicios como el diagnóstico del vehículo, sólo dispositivos autorizados pueden acceder a la Unidad Central de Comunicación del vehículo, si dispositivos malignos copian esa autorización, podrían manipular la Unidad Central de Comunicación de un vehículo. [41]

2.5.2.5.1.5.2 Duplicación No Autorizada de un Vehículo y una RSU

Una vez que el atacante obtiene los ID del vehículo y del RSU, estos pierden su imputabilidad. [41]

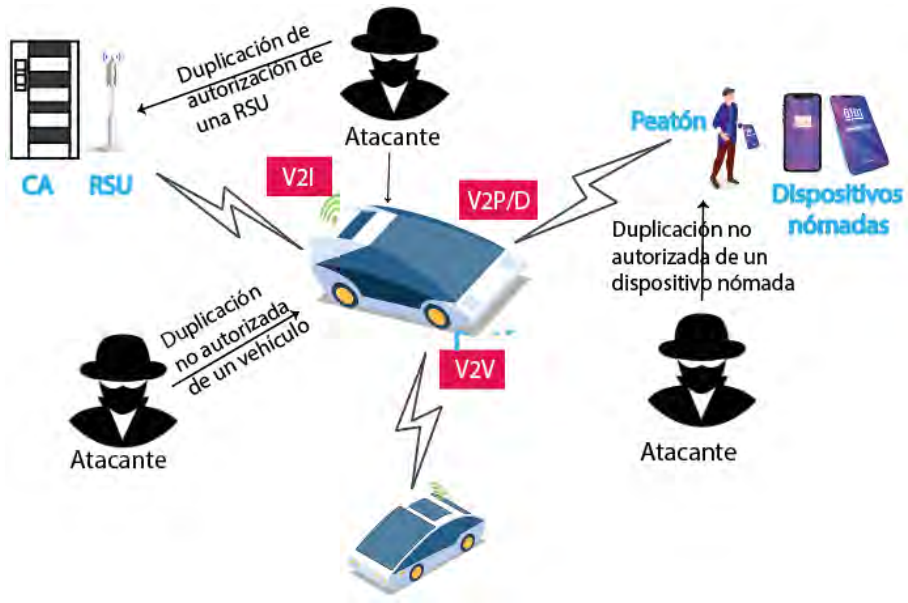


Figura 67 Amenazas a la Imputabilidad. Fuente: UIT-T (2020) [41]

2.5.2.5.1.6 Amenazas a la Autorización

2.5.2.5.1.6.1 Acceso no Autorizado a la información de Seguridad de un Vehículo

Es la misma definición de explotación de confianza. Para manipular, borrar y reescribir los datos de Seguridad del vehículo incluidos los parámetros específicos de los vehículos como el registro del sistema o el umbral del freno (ver Figura 68). [41]

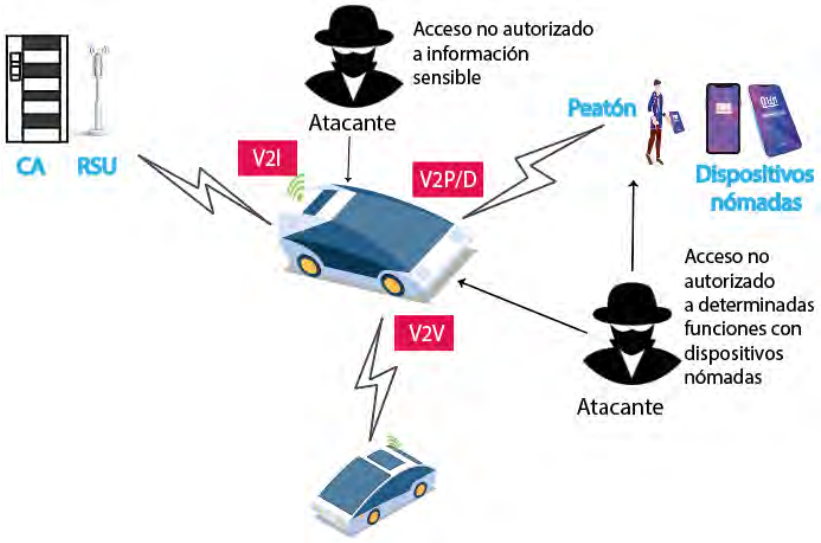


Figura 68 Amenazas a la Autorización. Fuente: UIT-T (2020) [41]

2.5.2.5.1.7 Estándares

IEEE 1602.9 Para la Seguridad de comunicaciones vehiculares. [14]

2.5.2.6 Otras amenazas

2.5.2.6.1 MIMO Masivo

El número de antenas MIMO Masivo en la gNB al ser alto, no es posible decodificar la mayoría de los símbolos originales provocando interferencias, mientras que los usuarios legítimos pueden recuperarlos con un solo número de antenas limitados. [31]

2.5.2.6.2 Botnets

"Los dispositivos móviles 5G admitirán diferentes opciones de conectividad y un mayor Ancho de Banda de UL y tendrá que estar siempre encendido y conectado a Internet. Así los futuros atacantes estarán habilitados en implementar Botnets Móviles para redes de Comunicación 5G en muchas formas eficientes (ver Figura 69)." [37]

Un Botnet Móvil 5G Centralizado consta de:

2.5.2.6.2.1 Bot – Master

"Podrá acceder y gestionar el Botnet de forma remota a través de los servidores Bot – Proxy, es decir, los servidores centrales de C&C. Los Bot – Master se encargarán de elegir los dispositivos móviles que estarán comprometidos por Malware y convertido en Bots. El Bot - Master explotará las vulnerabilidades de Seguridad por ejemplo el Sistema Operativo y las vulnerabilidades de configuración de los dispositivos móviles elegidos." [37]

2.5.2.6.2.2 Servidores Bot – Proxy

"Será el medio de comunicación que el Bot – Master utilizará para comandar y controlar los Bots indirectamente." [37]

2.5.2.6.2.3 Bots

"Serán programados e instruidos por el Bot – Master para realizar una variedad de actividades maliciosas, como la Denegación de Servicio Distribuida (DDoS) ataques contra elementos de la Red en la Red Móvil, Distribución Masivo de Spam, robo de datos confidenciales, mayor distribución, así como la instalación de Malware en otros dispositivos Móviles." [37]

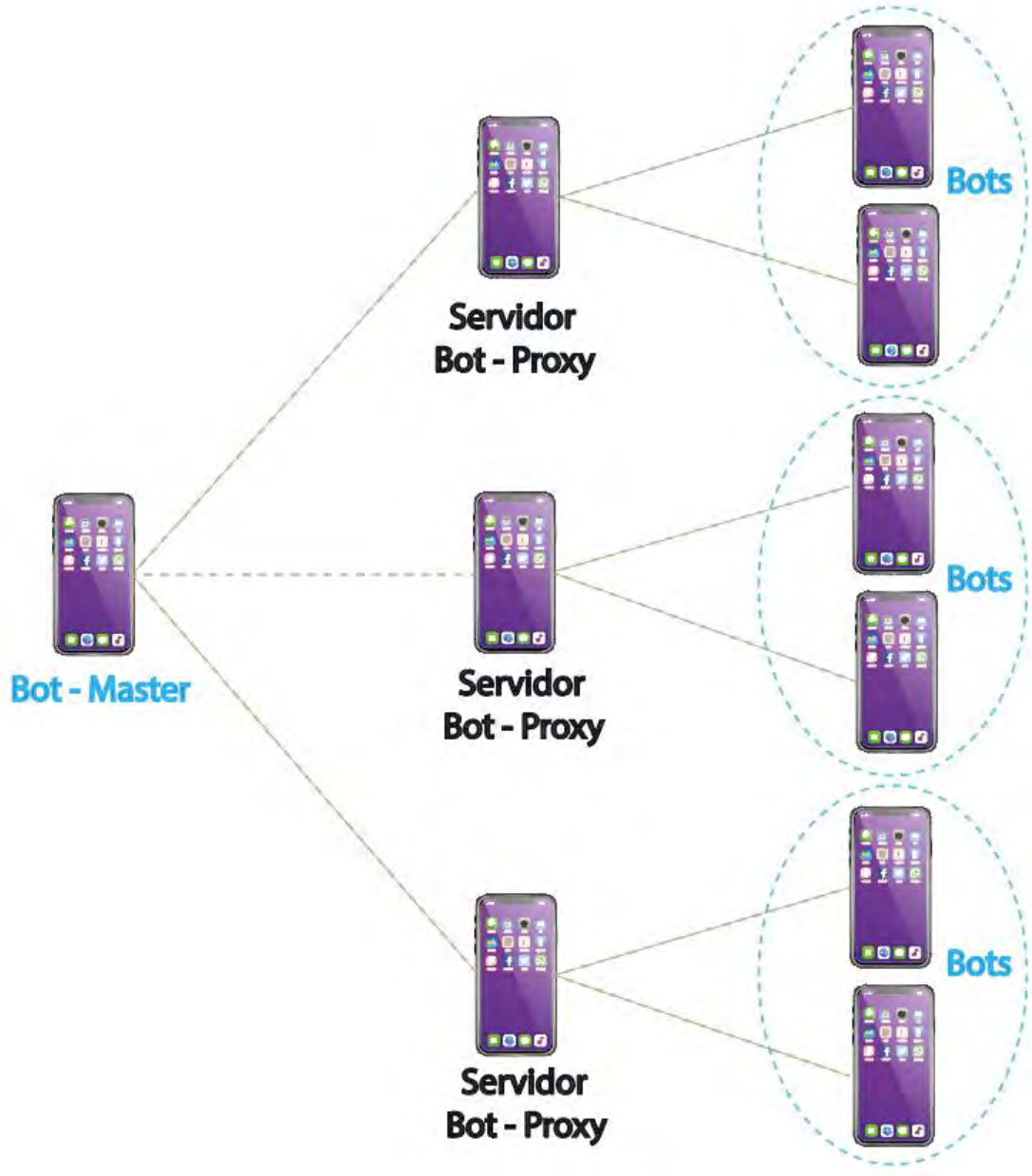


Figura 69 Botnets Móviles 5G Centralizados. Fuente: Jonathan Rodriguez, Georgios Mantas, Nikos Komninos, EvaristeLogota, Higo Marques (2015) [37]

2.6 Medidas básicas de protección 5G

2.6.1 Mitigando las Amenazas de 5G autónomo

Algunos elementos de una Arquitectura de Seguridad 5G tenemos, (ver Figura 70)

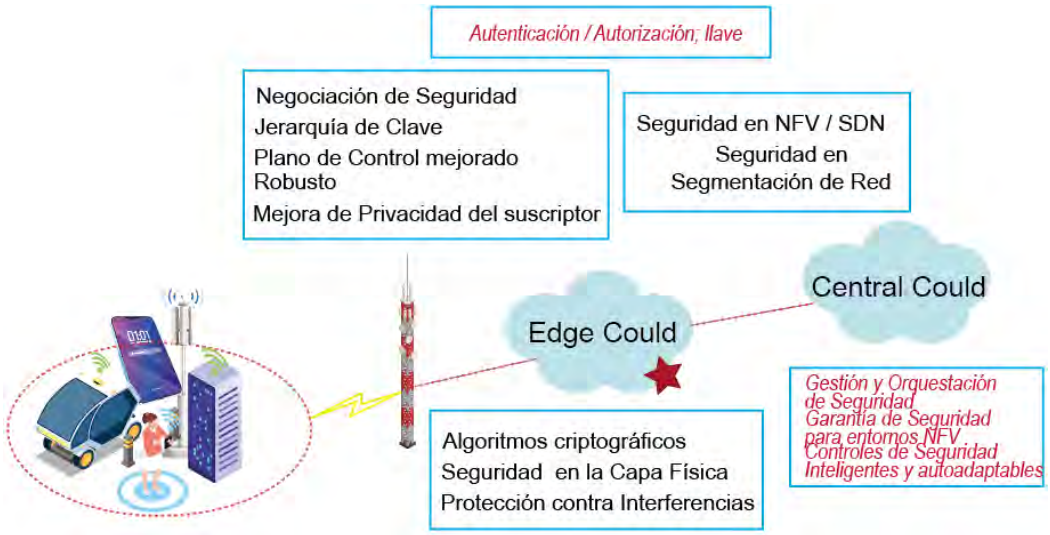


Figura 70 Elementos de una arquitectura de Seguridad 5G. Fuente: Dongfenf fang, Yi Qian, Rose Qingyang Hu (2018) [31]

Tabla 56 Medidas de protección ante amenazas de 5G Autónomo. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021 [30]

Amenazas	Medida de protección
UE	La Autenticación solida es la mejor solución para este tipo de ataque. Para lograr una autenticación de manera rápida, el uso de SDN de alta flexibilidad y programabilidad. [30]
Ataque de Hombre en el Medio (MitM)	La implementación de Seguridad de Integridad en el Plano de Usuario requiere de muchos recursos afectando el rendimiento del usuario. IP está habilitada para los mensajes en el Plano de Usuario, pero no de Control. [30]

	El tráfico de datos es vulnerable porque 5G tiene dividida el Plano de Control con el de Usuario. [30] “El controlador SE – Floodlight proporciona mecanismos para la separación de privilegios al agregar una API programable segura, funciona como mediador entre la aplicación y el Plano de Datos. Verifica las reglas de flujo generadas por las aplicaciones e intenta resolver los conflictos de reglas de flujo de aplicaciones.” [20] Para mitigar riesgos de fallas de controlador debido a la escalabilidad, incluye Redundancia, maximizando sus capacidades de almacenamiento y procesamiento. [20]
SDN y NFV	• IPSec [30] • Capa de Transporte TLS para proteger esa comunicación.[30] • Protección de interfaces y funciones de Segmentos de Red. [19] • Protección contra la selección fraudulenta de Segmentos de Red. [19] • Evitar el acceso no autorizado a una instancia de Segmento de Red. [19] • Uso de diferentes protocolos y Políticas de Seguridad de diferentes Segmentos de Red. [19] • Uso de diferentes procedimientos de autenticación y autorización de inquilinos de diferentes segmentos. [19] • Protección contra ataques DoS contra recursos compartidos por múltiples sectores. [19] • Evitar los ataques con otros sectores utilizando el mismo Hardware. [19] • Las funciones de Seguridad tienen en cuenta las funciones de Red Física y virtual. [19] • Aislar los Segmentos de Red, incluso si el mismo UE está conectado a ambos al mismo tiempo [19]

Amenazas RAN	El identificador SUPI evita según la 3GPP que un atacante rastree un objetivo que afecte la privacidad de los suscriptores. [30] Inclusive MIMO garantiza la integridad de la información operando en el espectro de onda milimétrica (mmWave). [30]

2.6.1.1 Mitigando las Amenazas según CISA

Tabla 57 Medidas de protección según CISA. Fuente: Homeland Security (2020) y datos adicionales. [19][39]

Medida de Protección	Descripción
Fomentar el desarrollo continuo y confiable de tecnologías, servicios y productos 5G	Inversión para la fabricación y compra de componentes confiables aumentarán la producción confiable y reducirán los Riesgos de tecnologías maliciosas que no son confiables. [39]
Fomentar el desarrollo continuo y confiable de las próximas generaciones de tecnologías de comunicaciones	"Las tecnologías y estándares 5G se basarán en el desarrollo continuo de mejoras de Seguridad, en este caso USA pretender hacer la inversión nacional, disminuyendo potencialmente la influencia de las naciones adversarias y disminuyendo la dependencia de USA de tecnologías no confiables." [39]
Promover estándares y procesos internacionales que sean abiertos, transparentes e impulsados por el consenso y no pongan en desventaja	Los Organismos de Normalización como 3GPP e UIT deben promover los estándares relacionados con 5G actualmente adoptados e impulsar su desarrollo. [39]

a las empresas TIC de confianza.	
Limitar el uso de equipos 5G con vulnerabilidades conocidas o sospechas	Por ejemplo, “el gobierno de Estados Unidos de América se encuentra limitando la adopción de equipos 5G que pueden contener vulnerabilidades a través de la Sección 889 de la Ley de Autorización de Defensa Nacional de 2019, la Ley Federal de Seguridad de la Cadena de Suministro de Tecnología y Servicios de Información y Comunicaciones. “[39]
Comprometerse con el Sector Privado en la Identificación de Riesgos y los esfuerzos de mitigación	“El Sector Privado puede ayudar a mitigar las vulnerabilidades de 5G proporcionando información de apoyo en el desarrollo de mejores prácticas.” [39]
Garantizar capacidades de Seguridad sólidas para aplicaciones y servicios 5G	El Gobierno de USA adoptarán un enfoque centrado en la prevención desarrollando capacidades de Seguridad que no sólo protejan la infraestructura 5G, sino también las aplicaciones y servicios que las utilizan, mitigando el riesgo de Malware que se transporte a través de dispositivos protegidos y se defenderá contra el comando y control no autorizados de dispositivos conectados explotados.” [39]
Seguridad de la Red	• Uso de técnicas de Cifrado de datos y transporte de datos. [19] • Medidas para protegerse contra ataques DoS y DDoS. [19] • Protección contra la suplantación de IP. [19] • Deshabilitar servicios no utilizados. [19]

	• Uso de filtros de etapas múltiples y controles adaptivos para limitar el daño. [19] • Prevención de la manipulación de rutas entre dominios. [19] • Análisis del tráfico para detectar ataques o errores y toma de protección adecuadas. [19] • Supervisión de la infraestructura para identificar y prevenir las amenazas de forma continua. [19] • Controlar la Red en relación con los sistemas infectados de los clientes. [19] • Cooperación con proveedores de anti – Malware. [19] • Asegurar la disponibilidad de números de emergencia. [19]
Arquitectura de Red	• Asegurar el hardware. [19] • Comunicación cifrada a través de Interfaces y API • Procedimientos sólidos de Autenticación y Control de Acceso. [19] • Selección cuidadosa de empleados, así como la transparencia y trazabilidad en el día a día. [19] • Trabajar de acuerdo con las mejores prácticas, monitorear las medidas de Seguridad, aplicar parches y mejoras de Seguridad, realización de análisis de vulnerabilidades. [19] • Cifrado de datos sólidos, mecanismos para generador de claves. [19] • Autenticación de dos o múltiples factores y monitoreo proactivo no autorizados. [19]

	• Divulgación de registros y datos, detalles de la Infraestructura como la situación del parche y Firewalls, así como la información sobre el monitoreo y las alarmas para el inquilino, el proveedor de servicios, por parte del proveedor de la nube. [19]

2.6.1.2 Medidas de Protección según Dongfeng, QingyangHu y Qian

Tabla 58 Medidas de protección ante ataques en Redes Inalámbricas según Dongfeng Fang, Rose QingyangHu, Yi Qian (2018) [31]

Amenazas	Medida de protección
Escuchas clandestinas	El cifrado de señales a través de un enlace de Radio. [31] El actor malicioso no pude interceptar la señal recibida directamente debido al cifrado. Aunque depende de la fuerza del Algoritmo de Cifrado y la capacidad informática del actor para demostrar su refuerzo y efectividad. [31]
Análisis de tráfico	Método de cifrado. [31]
Interferencias	Técnicas de método ensanchado como: • Espectro Ensanchado de Secuencia Directa (DSSS) • Espectro Ensanchado por el Salto de Frecuencia (FHSS) Como métodos de comunicación seguros. [31]
Relé	“Se puede utilizar para ayudar al remitente a asegurar la transmisión de la Señal,” [31] juntamente con múltiples antenas, disminuyendo la probabilidad de escuchas clandestinas. [31] Se proponen dos protocolos de selección de relés: • La selección de Relés Óptima (ORS).

	• La selección de Relés Parciales (PRS).
Ruido Artificial	"Se puede integrar Ruido Artificial a una señal para asegurar su transmisión deseada." [31] Proporcionando Confidencialidad de los Datos. [31]
Procesamiento de señales	Para el procesamiento de señales se puede utilizar el esquema de Transmisión Segura (OSPR), de Transmisión Multipunto Coordinada Dinámica (CoMP) y MIMO Masivo. [31] • El esquema de Transmisión segura a través de Símbolos de Fase Rotada (OSPR) con un número ilimitado de antenas en una Celda. [31] La Estación Base gira aleatoriamente la Fase de los Símbolos Originales antes que se envíen a los dispositivos de los usuarios emisores correctos. • Los actores malintencionados no pueden interceptar las señales, sólo los usuarios a quien va dirigido, inclusive interferir con las rotaciones de Fase correctas para recuperar los símbolos originales. [31] • El Esquema de Transmisión Multipunto Coordinada Dinámica (CoMP) para la selección de la Estación Base mejora la cobertura de la señal. [31] Se aplica MIMO Masivo a Hetnets para asegurar la Confidencialidad de los Datos en presencia de múltiples intrusos, mejorando significativamente el rendimiento ante las escuchas clandestinas. [31]
Métodos criptográficos	Los métodos criptográficos se utilizan para implementar la Confidencialidad de los Datos mediante el cifrado de datos con claves secretas. La criptografía asimétrica se puede aplicar a distribuciones de claves para reducir el costo del cifrado, se adopta la criptografía simétrica. [31]

	Examine la página 3, encriptación simétrica.
Gestión de Claves	“Es el procedimiento o técnica que respalda al establecimiento y mantenimiento de relaciones de claves entre partes autorizadas, donde la relación de claves es la forma en que se comparten datos comunes entre entidades de comunicación. Los datos comunes pueden ser claves públicas o secretas, valores de iniciación y otros parámetros no secretos.” [31]
Privacidad	“Los flujos de datos para las Redes Inalámbricas 5G llevan una amplia información de privacidad de información de privacidad personal como la Identidad, posición, contenido privado. En algunos casos, la filtración de privacidad puede tener consecuencias graves.” [31] Dependiendo de los requisitos de privacidad de las aplicaciones, la protección de la privacidad es un gran desafío. Por ejemplo: Para proteger la privacidad de la ubicación y preferencias de los usuarios se propone un algoritmo descentralizado para la selección del Punto de Acceso. Para proteger la identidad del cliente de cifra con un pseudo identidad del cliente de origen con clave pública utilizando un método de cifrado sin certificado. [31]
Helnet	“Para hacer frente a los ataques de escucha clandestina se propone una política secreta de asociación móvil basada en la Potencia de Señal Recibida Promedio Truncada Máxima (ARSP).” [31] Para mejorar la cobertura de comunicación en Helnet se puede aplicar la Transmisión Multipunto Coordinada (CoMP). Sin embargo, puede aumentar el riesgo de que los usuarios legítimos lo escuchen a escondidas, pero el umbral de selección de Estaciones Base puede mejorar el rendimiento de la cobertura segura.” [31]

	Para proteger la información de ubicación del usuario, se propone un algoritmo diferencial privado Gale-Shapley para evitar la filtración de información con cierta QoS para los usuarios. [31]

2.6.1.3 MIMO y BotNets

Tabla 59 Medidas de protección para MIMO y Botnets. Fuente: Elaboración propia basado en [30][31]

Amenazas	Medida de protección
MIMO Masivo	Formación de Haces. Véase la página 87 y 90. [31]
Botnets de IoT	Según 3GPP, la mejor opción es Cifrado IPSec evitando ataques desde Internet o Bots que podrían afectar significativamente aplicaciones IoT. [30]

2.6.1.4 Según Cisco Netacad

Tabla 60 Medidas de protección según cisco Netacad. Fuente: [1]

Medida de protección
Es posible realizar ciertas técnicas para mitigar los ataques en conjunto o de manera individual, entre ellas se encuentran: Desactivar las cuentas después de un número específico de intentos fallidos de acceso. [1] Uso de contraseñas seguras que contengan más de 8 caracteres con una combinación de números letras mayúsculas y minúsculas, caracteres especiales. cambiándolo cada semana. [1]

- Vigilar el tráfico de manera recurrente. [1]
- Realizar copias de Seguridad y cifrar contenido. [1]
- Implementar software de Seguridad como Firewalls, instalar VPN, Red Privada Virtual y antivirus. [1]

2.6.2 Seguridad para la Red

2.6.2.1 Funciones del ciclo de vida de Seguridad para Redes y Sistemas Móviles

2.6.2.1.1 Gestión Segura de Dispositivos

"Herramientas como MDM ayudan a las organizaciones a hacer cumplir las Políticas de Seguridad, protegerse contra amenazas maliciosas y restringir el acceso no autorizado a dispositivos móviles. Dichas políticas pueden hacer cumplir los mecanismos de protección para dispositivos móviles, como la aplicación de códigos de acceso alfanuméricos complejos." [20]

2.6.2.1.2 Monitoreo de Seguridad

Visibilidad en tiempo real para ofrecer una garantía de servicio y proteger las infraestructuras de Red ante amenazas a la Seguridad. [20]

"Las soluciones de monitoreo ofrece la capacidad de inspeccionar tanto la señalización como el tráfico de Datos en múltiples puntos de la Red, como los Protocolos utilizados." [20]

"Los Sistemas de Detención de Intrusiones (IDS) y los Sistemas de Prevención de Intrusiones (IPS) observan el tráfico de la Red de acuerdo con diferentes Políticas de Seguridad, encontrando vulnerabilidades, ataques y amenazas." [20]

2.6.2.1.3 Resistencia de la Red

“La Red debe ser apta para proporcionar servicios a los usuarios cuando se presenten, a pesar de sufrir diversos desafíos de Seguridad. [20] Estas incluyen defender, recuperar, diagnosticar y perfeccionar.

2.6.2.1.4 Automatización de la Seguridad de la Red

“Para la adquisición, análisis de Información, selección de decisiones y acciones, así como su implementación.” [20]

2.6.2.2 Dominios de Seguridad de la Arquitectura de Red 3GPP

2.6.2.2.1 Seguridad al Acceso a la Red

“Incluyen las Funciones de Seguridad que permiten UE o ME para autenticar servicios de Red y acceder de forma segura. Para lograrlo intercambian mensajes con la Red de Servicio. [19]

2.6.2.2.2 Seguridad en el Dominio de Red

“Incluyen las Funciones de Seguridad que permiten nodos de trabajo para intercambiar de forma segura mensajes de señalización y datos de usuario. [19]

2.6.2.2.3 Seguridad en el Dominio de Usuario

“Protege el acceso a los usuarios a dispositivos y servicios móviles. También incluye mecanismos de Seguridad basados en Hardware.” [19]

2.6.2.2.4 Seguridad en el Dominio de Aplicación

“Las funciones de Seguridad ubicadas aquí, garantizan la comunicación segura de aplicaciones, tanto del usuario como del proveedor.” [19]

2.6.2.2.5 Seguridad en el Dominio de la SBA

"Seguridad con las NF y sus interfaces. También se tiene en cuenta la Itinerancia entre la Red doméstica HE y la Red visitada SN." [19]

2.6.2.2.6 Visibilidad y Configurabilidad de Seguridad

"Permiten a los usuarios estar informados sobre el estado operativo de las medidas de Seguridad y solicitar funciones de Seguridad si es necesario." [19]

2.6.2.3 Seguridad del Enlace de Datos

Con el uso de TLS y DTLS. [20]

2.6.2.4 Seguridad en Redes Inalámbricas desde la perspectiva de Servicios de Seguridad

Como se ha dicho anteriormente en la página 11, "Seguridad de la información abarca todos los estados o formas de diferentes riesgos que se enfrenten, independientemente si se encuentran interconectados o no." [1][3] Por lo tanto, Ciberseguridad está dentro de Seguridad de la información. Los servicios de Seguridad de Redes Inalámbricas aplican para los servicios de Seguridad convencionales. [20]

Los servicios de Seguridad en Redes Inalámbricas se encuentran en las páginas 10 y 11.

Tabla 61 Seguridad en Redes Inalámbricas desde la perspectiva de Servicios de Seguridad y recomendaciones de Seguridad del UIT-T [20] [31]

Amenazas	Medida de protección
Autenticación	Hay dos tipos de autenticación: de entidad y mensaje. La Autenticación de entidad se utiliza para identificar quien solicita un servicio. [31] Utiliza la Gestión de Autenticación híbrida y flexible y se pueden implementar en tres formas diferentes:

	• Por Red • Por proveedores de servicio • Por Autenticación por Red y proveedores de servicio. Debido a la velocidad de datos muy alta y latencia baja se espera que la Autenticación 5G sea más rápida. [31] Al ser más rápidas, el esquema de autenticación rápida basado en SDN es la mejor opción, ya que tiene un mejor rendimiento de retardo debido a la flexibilidad y programabilidad de SDN en Redes 5G. [31]
Confidencialidad	La Confidencialidad consta de dos aspectos; de datos y privacidad. [31] De datos protege la transmisión de los datos de ataques pasivos al limitar el acceso solamente a usuarios legítimos. [31] La privacidad evita el flujo de datos descontrolado en Redes 5G. [31] El cifrado de datos se ha utilizado ampliamente para asegurar la Confidencialidad de los datos en Redes 5G, al evitar que los usuarios no autorizados extraigan Información útil al transmitir. [31] *Se puede utilizar los dos tipos de cifrado. Véase la página 3 la encriptación simétrica y en la página 215 asimétrico.* Control de Acceso y permisos de archivos para garantizar la Confidencialidad de los datos. [20]
Disponibilidad	Evalúa que tan robusta es el sistema cuando se enfrenta a varios ataques y es una métrica clave de rendimiento en 5G, garantizando comunicaciones ultra confiables. [31] “Para mitigar los ataques DoS y ofrecer disponibilidad se ha propuesto un Sistema secreto de salto de frecuenta adaptativo como posible técnica 5G basado en una plataforma de Radio Definida por Software. El estimador de Tasa de Error de Bit (BER)

	basado en la información de la Capa Física se aplica para decidir la lista negra de Frecuencias bajo el ataque DoS.” [31] Para reducir la Tasa de Conmutación y la probabilidad de Interferencia, se propone un esquema antiinterferencia de salto de tiempo pseudoaleatorio para usuarios cognitivos en 5G para contrarrestar los ataques de Interferencia. [31] *Véase la Figura 67, el diagrama de bloques de un sistema de salto de tiempo pseudoaleatorio.*
Control de Acceso	“Medida de Seguridad que garantiza que sólo el personal o dispositivos autorizados accedan a los recursos de la Red.” [20]
No repudio	“Asegurarse que un usuario o dispositivo específico haya realizado una acción en particular.” [20]
Integridad de los Datos	“Asegura la exactitud de los datos en la transmisión y los protege de modificaciones, borrado, creación y replicación no autorizados.” [20]

2.6.3 Algoritmos 5G

Tabla 62 Algoritmos de Cifrado para encriptación 5G. Fuente: Jyrki T. J. Pennttinen (2019) [18]

Algoritmo	Descripción
NEA0	Algoritmo de Cifrado Nulo.
128-NEA2	35.215 Algoritmo basado en AES de 128 bits en modo CTR.
128-NEA3	Algoritmo basado en ZUC de 128 bits como se hace referencia en 3GPP TS.35221.

En la Tabla 62 se resume los Algoritmos de Cifrado para la encriptación 5G. La Tabla 63 los Algoritmos de Protección de Integridad. [18]

Tabla 63 Algoritmos de Protección de Integridad. Fuente: Jyrki T. J. Pennttinen (2019) [18]

Algoritmo	Descripción
NIA0	Algoritmo de Protección de Integridad Nula.
128-NIA2	Algoritmo basado en AES de 128 bits en modo CMAC.
128-NIA3	Algoritmo basado en ZUC de 128 bits como se hace referencia en 3GPP TS.35.221.

"El UE y la Red de servicio negociarán el Algoritmo utilizado en función de las políticas y estándares 5G, así como las capacidades de Seguridad. Esto aplica a la protección del Cifrado e Integridad de la Señalización RRC." [18]

2.6.4 Arquitecturas de Seguridad

2.6.4.1 Autenticación basado en SDN

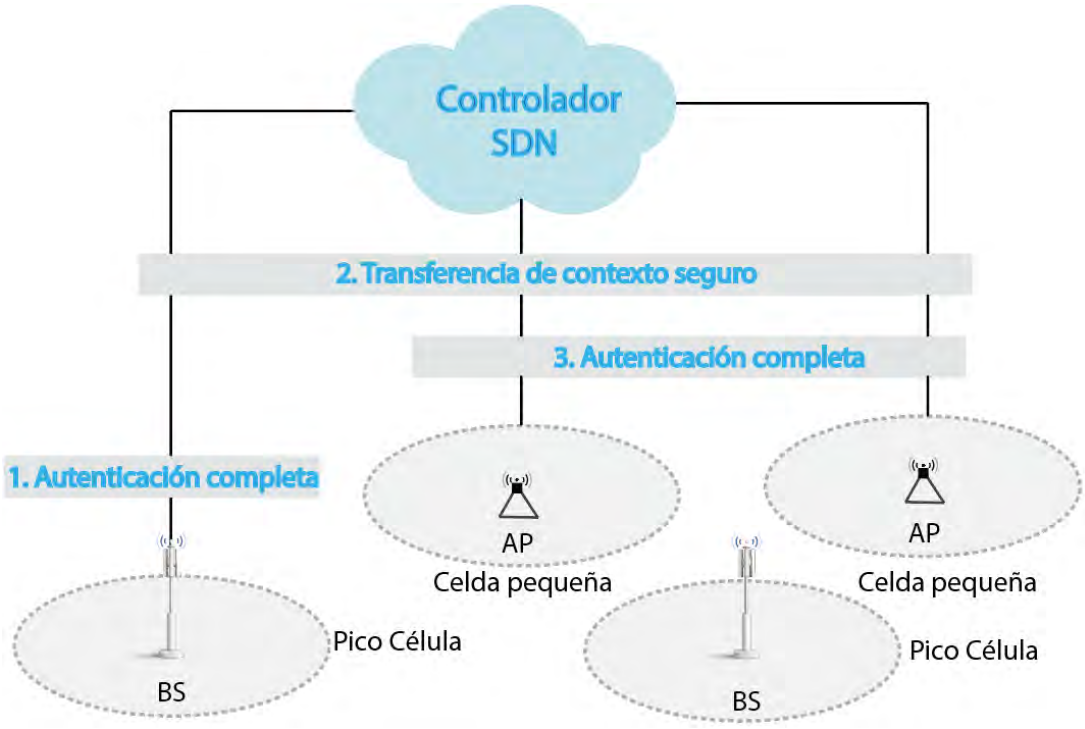


Figura 71 Modelo de Autenticación habilitado para SDN. Fuente: Dongfeng Fang, Yi Qian., Rose Qingyang Hu., (2018) [31]

“(Ver la Figura 71,) el controlador SDN implementa un modelo de Autenticación para monitorear y predecir la ubicación del usuario con el fin de preparar Celdas relevantes antes de la llegada del usuario.” [31]

2.6.5 IoT

La protección de los ciudadanos con tales amenazas pone en evidencia el desafío que provoca, ya que los Ciberataques cada vez son más sofisticados. Esto se puede solucionar aumentando la vigilancia cibernética y resguardar los datos con medidas de protección eficientes. Por lo tanto, el IoT también se puede interpretar como un componente elemental en el mundo cibernético y todos necesitan un nivel adecuado de conocimiento de los distintos ataques y lo métodos de protección respectivos para poder sobrevivir en nuestro entorno. [18]

Ver página 10 con el tema: "Seguridad Cibernética."

2.6.5.1 Realización de un IoT Pentest

Debido a los Riesgos que se presentan como la Cadena de Suministro, es necesario realizar una prueba de Pentest de IoT. Es una evaluación que se realiza a varios componentes IoT para detectar posibles vulnerabilidades que pondrían en riesgo la CIA de los datos. [8]

El proceso para realizar la verificación se da mediante el alcance y la metodología deseada, comienza con el mapeo de superficie de ataque para llegar a la solución, seguida con la identificación de las vulnerabilidades, la realización de exploración y post explotación y finalmente con un informe técnico en profundidad. [8]

2.6.5.1.1 Mapeo de Ataque

Significa explotar todos los posibles puntos de entrada que probablemente podría abusar potencialmente y organizarlos en la arquitectura de los componentes para llegar a la solución. [8]

2.6.5.1.2 Identificación de Vulnerabilidades

2.6.5.1.2.1 Dispositivos Integrados

Según el caso de uso para monitorear, analizar datos o acciones, en dispositivos integrados *Algunas vulnerabilidades encontradas en IoT pueden verse en la página 179.*

2.6.5.1.2.2 Firmware, Software y Aplicaciones

Examinación del Firmware y los componentes que estructuran un dispositivo IoT encontrando sus vulnerabilidades. [8]

Véase en la página 180 las vulnerabilidades de los componentes IoT.

2.6.5.1.2.3 Comunicaciones por Radio

Algunos protocolos que se utilizan en los dispositivos IoT son Celulares, Wi-Fi, BLE, ZigBee, Wave, 6LoWPAN, Lora y más.” [8] dependiendo del protocolo se requiere hardware como herramienta para poder realizar su análisis. [8] *Algunos ejemplos de vulnerabilidades encontradas, página 181.*

2.6.5.1.2.4 Exploración Simulada por Atacantes

2.6.5.1.2.4.1 División de Equipos por Áreas

“El equipo de Software Defined Radio (SDR) encargados de la explotación de la comunicación por Radio y el equipo de Pentest de Software trabajando en Firmware, aplicaciones móviles, aplicaciones Web y activos basados en la nube.” [8]

En conjunto para simular como un atacante en diversas perspectivas podría interferir maliciosamente en los dispositivos. [8]

2.6.5.1.2.5 Remediación

Trabajo con desarrolladores, ofreciéndoles soporte en el análisis y vulnerabilidades encontradas para que tenga solución inmediata. [8]

2.6.5.1.2.6 Revaloración

Posteriormente después de la mejora, se repite el proceso de exploración para verificar si las soluciones dadas son correctas o requieren de nuevos procesos de mejora. [8]

2.6.5.1.2.7 Análisis de Hardware

Su análisis ayuda a comprender mejor al dispositivo en general y su funcionamiento. [8]

2.6.5.1.2.7.1 Trabajar con el Dispositivo Real

Comenzar a trabajar con el dispositivo desde sus especificaciones. [8]

2.6.5.1.2.7.2 Encontrar Puertos de Entrada y Salida

Para comprender como funcionan los puertos. [8]

2.6.5.1.2.7.3 Inspección Interna

Implica abrir el dispositivos y mirar sus componentes e identificar las posibles superficies de ataques. [8]

2.6.5.1.2.7.4 Analizar Hojas de Datos

Verificación de información técnica esquemas del dispositivo, junto su ID de FCC[59]. [8]

2.6.5.1.2.7.5 Verificación de Componentes

Revisión de dispositivos integrados, chipset de Radio. [8]

[59] Comisión Federal de Comunicaciones. Regulador de dispositivos que emiten comunicaciones de Radio. [8]

2.6.5.1.2.7.6 Comunicación UART[60]

Es una Interfaz de comunicación, la capacidad de interactuar con UART es necesaria para obtener la Shell raíz no autentificado y el acceso al gestor de arranque. [8]

2.6.5.1.2.7.7 Comunicación Serial

El intercambio de datos entre los componentes. [8]

2.6.5.1.2.7.8 Radio Definido por Software

Responsable para que los dispositivos se comuniquen entre si e intercambien datos de manera inalámbrica. Se analizan las frecuencias, amplitud, modulación, ganancia y terminologías que se encuentran en “Glosario” al final del documento, con ayuda de herramientas que se instalan exclusivamente en Ubuntu. [8]

2.6.5.1.3 Post Exploración

Analizar los datos de las vulnerabilidades y medidas de Seguridad implementados en los dispositivos con la selección de herramientas y hardware especializados para analizar cada parte de los dispositivos. [8]

2.6.5.1.4 Informe Técnico

Es el registro de los resultados obtenidos de la exploración realizada y el análisis de solución. [8]

[60] “Método de comunicación en serie que permite dos componentes diferentes se comuniquen entre sí.” [8]

2.6.5.2 Casos de uso

2.6.5.2.1 Vehículos autónomos

2.6.5.2.1.1 Servicios de Seguridad V2X

En esta sección se describe los requisitos de Seguridad de acuerdo con los servicios de Seguridad en Redes Inalámbricas. *Véase las páginas 10, 11, del Capítulo 1.*

2.6.5.2.1.1.1 Confidencialidad

Una identidad no autorizada no debe revelar los mensajes V2V, V2I, V2P o V2D, tampoco debe poder analizar el ID de una persona como el desplazamiento de ruta. [41]

2.6.5.2.1.1.2 Integridad

Los mensajes enviados V2X, la RSU o dispositivo nómada deben estar protegidos contra la modificación o supresión no autorizados. [41]

2.6.5.2.1.1.3 Disponibilidad

Una entidad debe proporcionar información en tiempo real con ayuda de algoritmos criptográficos. [41]

2.6.5.2.1.1.4 No repudio

Una entidad debe tener firmas digitales para el envío de información. [41]

2.6.5.2.1.1.5 Autenticidad

OBU y RSU con ID legítimo para las comunicaciones. [41]

2.6.5.2.1.1.6 Imputabilidad

Toda entidad debe detectar e impedir comportamientos indebidos de la OBU o sensores de los vehículos mediante la verificación de sus datos. [41]

2.6.5.2.1.1.7 Autorización

Control de acceso y autorización de las diferentes identidades que hacen posible la comunicación y efectivamente los servicios brindados, denegando o permitiendo el acceso a entidades específicas. [41]

2.6.5.2.1.2 Medidas de Seguridad para V2X

2.6.5.2.1.2.1 Criptografía para la autenticación de entidades y la confidencialidad de los mensajes

El procedimiento es similar a la Figura 3 página 3, un método de encriptación simétrico donde la clave de encriptación y desencriptación es la misma, pero también existe otro tipo, encriptación asimétrico, la clave para encriptar del transmisor es diferente a la clave para desencriptar y para que el emisor pueda leer el mensaje (ver Figura 72). [1] [41]

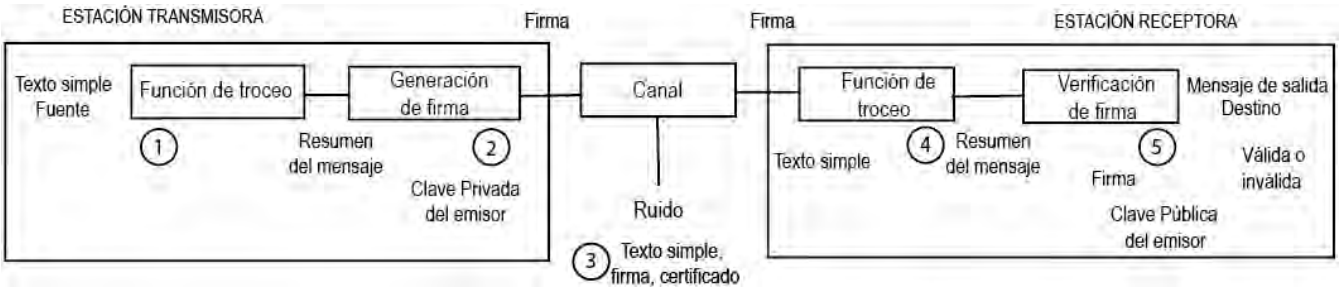


Figura 72 Generación y verificación de firmas. Fuente: UIT (2020) [41]

2.6.5.2.1.2.1.1 Procesamiento de generación y verificación de firma

- Paso 1: Desde un texto simple a enviar, con un algoritmo de generación numérica por ejemplo SHA-256 que es la función de troceo se calcula el resumen del mensaje del

texto mismo, a partir el Protocolo utilizado, carga útil, encabezado y la longitud de la cola. [41]

- Paso 2: Se genera una firma del resumen del mensaje que es el algoritmo de encriptación o clave privada del emisor(transmisor). [41]

- Paso 3: El texto simple, la firma y el certificado del transmisor se transmiten al receptor. [41]

- Paso 4: El receptor calcula el resumen del mensaje con el texto simple recibido del transmisor. [41]

- Paso 5: El receptor calcula un valor de verificación utilizando el resumen del mensaje del paso 4, la firma recibida y clave pública del transmisor. Si el valor de verificación es el mismo que el valor de la firma, la firma recibida es válida, si es deferentes es inválida y se descarta. [41]

2.6.5.2.1.3 Otras medidas de Seguridad V2X

El procedimiento de encriptación ECIES, desencriptación, la confidencialidad del mensaje para alertas de emergencia para Seguridad vial, autenticación para la comunicación para un grupo de vehículos, Seguridad con clave pública vehicular, se encuentran en la página 21 – 26 del libro [41]

2.6.5.2.2 Salud Móvil

“Se necesita altos requisitos de privacidad de los datos médicos mediante el uso de la técnica de cifrado de señales generalizado sin certificado (CLGSC), los autores propusieron un LRSA en un sistema de Salud Móvil.” [31]

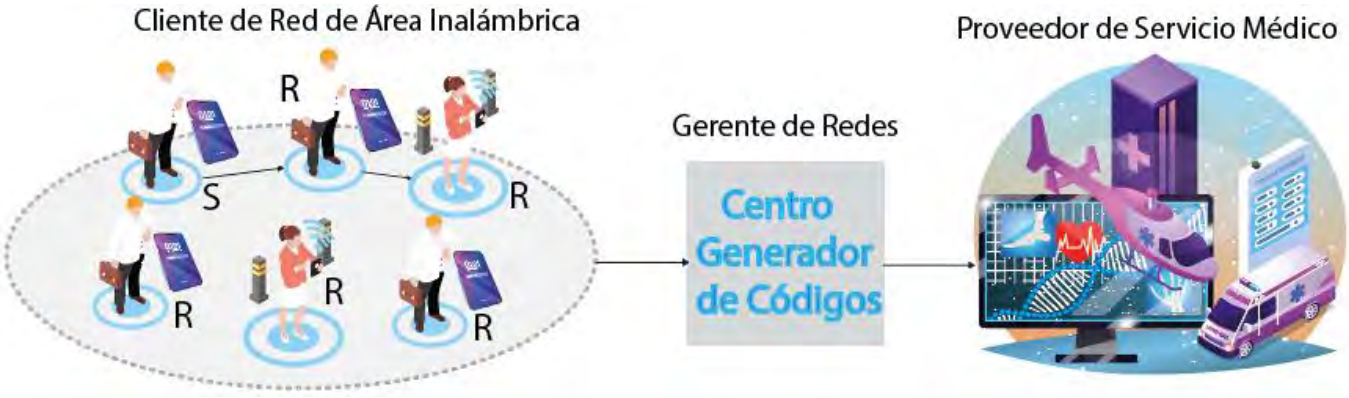


Figura 73 Modelo de un Sistema de Salud Móvil. Fuente: Dongfeng Fang, Yi Qian., Rose Qingyang Hu., (2018) [31]

"(Examine la Figura 73,) S indica el nodo de origen y R representa el nodo de transmisión. La autenticación anónima y mutua se implementa entre el cliente y el médico en una Red Inalámbrica para proteger la privacidad tanto de la fuente de datos como el destino propuesto. Con el método de encriptación asimétrico. [31]

2.6.5.3 Estándares de Seguridad IoT

- "ERC CIP 002 – 009 marco de Seguridad Cibernética para activos cibernéticos críticos.

- Pautas de NIST SP 800 – 53 para proteger activos cibernéticos críticos.

- Estándares de Cifrado FIPS 140 – 2 Nivel 2.

- Directrices NISTIR – 7628 para la Ciberseguridad de Redes Inteligentes." [18]

2.6.5.4 Herramientas de Simulación 5G más importantes

Tabla 64 Herramientas de simulación 5G más importantes. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

Simulador	Módulo	Proyecto	Lenguaje	Característica Clave

Netsim	5G NR (Tetcos, 2021)	Propietario Gratis	C	Versiones estándar / Pro. 5G NR herramienta basado en Release 15 / Serie 3GPP 38. De extremo a extremo simulación de Redes 5G. Apoyo a Funciones 5G Núcleo, 5G NSA, SDAP, PDCP, Capa MAC, Capa Física, espaciado, numerologías, estructura del marco y recursos físicos, agregación de operadores MIMO.
Ns – 3	5G – LENA (CTTC, 2021)	Open Source	C++	Módulo NS-3 para simular redes 3GPP 5G alineadas con NR Release 15 TS 38.300. Soporte RLC (TS 38.322), P DC P (especificación 38.323), MAC (TS 38.321, soporte de retardo de enlace ascendente), capa física (numerología, mini-ranura y formato de ranura UL-DL mixto, modelos de propagación y canal, formación de haces métodos, NR Abstracción PHY).
Matlab	5G Caja de herramientas (Math Works,	Propietario Gratis	C / C++	Herramienta de simulación de acuerdo con las especificaciones 3GPP 5G NR (versiones 15 y 16). Simulación de enlaces de comunicaciones 5G NR de extremo a extremo. Admite la capa física 5G NR (subportadora

	2021)			NR y numerología, canal de propagación modelos, canales y señales de enlace descendente y enlace ascendente, información de control y canales de transporte).
Open5G Núcleo	Open 5G Núcleo (Open5GCore, 2021)	Propietario Gratis	-	Kit de herramientas 5G basado en la funcionalidad de red principal 3GPP Release 15 y 16 (AMF, SMF, AUSF, UDM, NRF, UPF). Admite 5G NR y UE estándar [N1, N2, N3], diversidad de ruta de datos (PFCP [N4]), sesión avanzada gestión, segmento de red, acceso no 3GPP.
Simulador Vienna 5G	Sistema 5G (Muller et al., 2018)	Academic use license	Matlab	Simuladores basados en Matlab. multienlace, formas de onda (CP-OFDM, f-OFDM, FBMC, UFMC, WOLA), códigos de canal (LDPC, turbo, polar, convolucional), numerología flexible, propagación y modelos de canal.
Open 5GS	Open5GS (Open5GS, 2021)	Open Source	C	Herramienta de código abierto que implementa la red central de la red NR / LTE basada en Release-16.

2.7 Comparación de Seguridad de 4G y 5G

2.7.1 5G

2.7.1.1 Arquitectura de Seguridad del Sistema 5G

(Ver Figura 74)

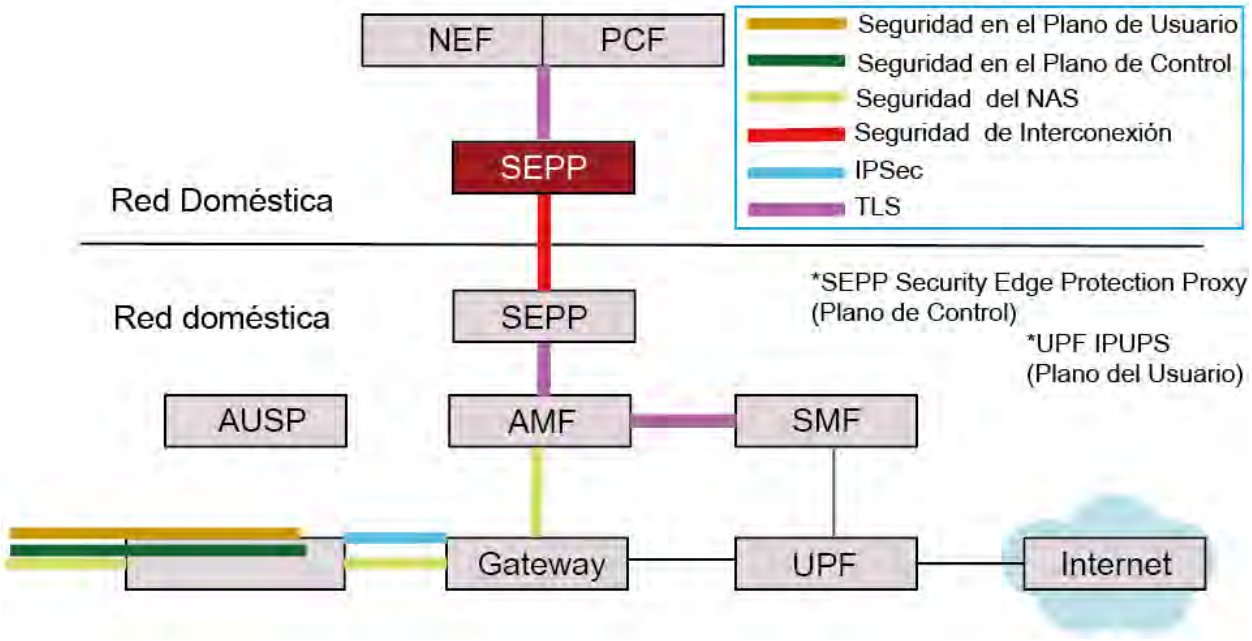


Figura 74 Arquitectura de Seguridad del Sistema 5G. Fuente: Cichonski Jeff (2020) [35]

Tabla 65 Requisitos de Seguridad para elementos de Red 5G y Funciones de Red 5G. Fuente: Ulrick Trick (2021) [19]

Elementos o Funciones de Red 5G	Requerimientos de Seguridad
UE	• Cifrado de señalización y datos de usuario entre UE y gNB por razones de Confidencialidad.

	• Garantizar la Integridad de los datos para la señalización y los datos de usuario entre UE y gNB. • Almacenamiento y procesamiento seguro de claves. • Cálculo de SUCI (Identificador Oculto de Suscripción).
gNB	• Cifrado de señalización y datos de usuario entre UE y gNB por razones de confidencialidad. • Garantizar la Integridad de los datos para la señalización y los datos de usuario entre UE y gNB. • Autenticar y autorizar un gNB durante la instalación y configuración. • Protección del Software gNB. • Protección de las claves utilizadas y almacenadas en el gNB. • Procesamiento y almacenamiento seguro de Datos de usuario y señalización. • Proporcionar un entorno seguro para todos los datos confidenciales. • Transmisión segura en la Interfaz F1 al dividir un gNB en CU y DU. • Transmisión segura de la Interfaz E1 al dividir una CU en CU-CP y CU-UP.
AMF	• Debido al cifrado de Confidencialidad de la señalización NAS. • Garantizar la Integridad de los datos para la señalización NAS
SEAF	• Activa la Autenticación a través de AMF en la Red de servicio. • Admite la Autenticación primaria del UE.
UDM	• Las claves a largo plazo para la autenticación y la asociación de Seguridad deben estar protegidas y no deben salir del

	entorno UDM / ARPF (Repositorio de credenciales de Autenticación y Función de Procesamiento). • Proporciona Servicio SIDF.
SIDF	• Responsable de resolver el SUPI del SUCI.
AUSF	• Procesa solicitudes de Autenticación para acceso 3GPP y no 3GPP. • Transfiere SUPI ala VPLMN (Red Móvil Terrestre Pública Visitada) después de una autenticación exitosa.
Red Principal en general	• Creación de zonas de confianza, en todo caso de distintos proveedores. • Descubrimiento seguro y registro de NF en la SBA. • Conexiones seguras de extremo a extremo para la Capa de aplicación entre Redes Centrales 5G.
NRF	• NRF y NF que solicitan un servicio, deben Autenticarse entre sí. • El NRF proporciona Autenticación y la Integridad de los datos entre NEF y AF (Función de la Aplicación). • Autenticación mutua. • No comunica información sobre el Segmento de Red o SUPI al exterior.
NEF	• Garantiza la Confidencialidad y la Integridad de los datos entre NEF y AF (Función de Aplicación.) • Autenticación mutua. • No comunica información sobre el Segmento de Red o SUPI al exterior.
SEPP Security Edge	• Proteger las entidades internas del Plano de Control. • Autenticación mutua con el SEPP correspondiente.

Protection Proxy	

2.7.2 4G

2.7.2.1 Arquitectura de Seguridad del Sistema 4G

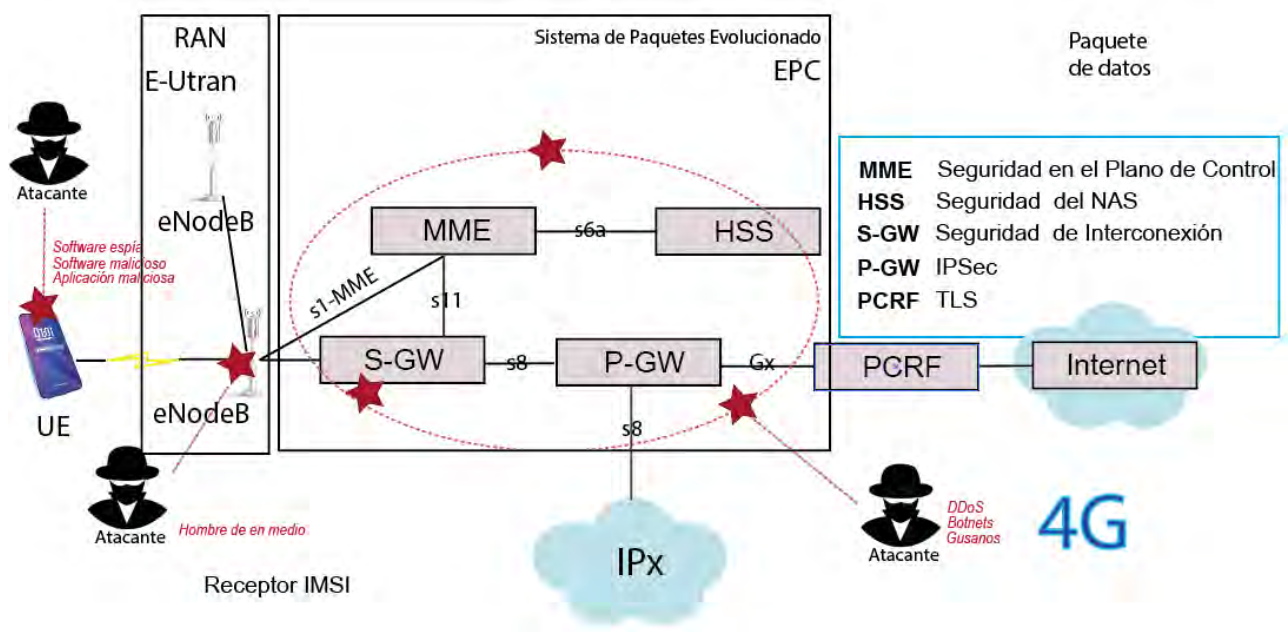


Figura 75 Panorama de Amenazas de Seguridad de extremo a extremo 4G. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018 [20]

Examine la página 67, “Amenazas y Seguridad específicas para la Cuarta Generación Móvil, Tabla 24. Resume las Amenazas de Seguridad y las Medidas de Seguridad exclusivas para esa generación.

Página 54, Tabla 17 Resumen de los componentes de las Arquitecturas de las Generaciones Móviles, Figura 20 “La evolución de la Red Móvil y los elementos de apoyo, página 55. Descripción detallada del funcionamiento de la 4ta Generación Móvil página 56 y 57 incluyendo Tabla 18 y Figura 21, Figura 70 tomada como referencia a la Figura 57, página 156 como ejemplo de Amenazas de Seguridad de Extremo a extremo.

Se determina que 4G y 5G no cuenta con ninguna similitud entre las funciones de Red, por lo tanto, en ese aspecto, no se puede realizar una comparativa de Seguridad basado en esos elementos, al menos que sea a nivel general.

Examine página 67.

2.7.3 Diferencias entre servicios brindados de Seguridad en Redes Inalámbricas de ambas generaciones móviles

Tabla 66 Diferencias entre servicios brindados de Seguridad en Redes Inalámbricas, 4G y 5G. Fuente: Elaboración propia basado en: [7][18]][20][30][31][35][40][42]

Diferencias	4G	5G
Autenticación	Si hacemos una comparación entre 4G LTE. El acuerdo de Autenticación y clave AKA se basa en claves asimétricas. [31]	Sin embargo, 5G requiere Autenticación no solo entre UE y MSC sino también de los proveedores de servicio. [31]
Confidencialidad	"Deliberadamente no discutimos las defensas para los ataques observados, ya que al agregar retrospectivamente la Seguridad en un Protocolo existente sin romper la compatibilidad hacia atrás, a menudo se obtienen soluciones que no se sostienen bajo un escrutinio extremo." [7]	El servicio de privacidad 5G Autónomo, merece mucha más atención que en las redes celulares heredadas debido a las conexiones masivas. [31]

Amenazas de Seguridad específicas y adicionales.	• Sistema Operativo parchado y actualizado. [20] • Instalación de antivirus. [20] • Problemas de Itinerancia. [20] • Cifrado en dispositivos móviles. [20] • Sin protección de Integridad en el Plano de Usuario. • Seguimiento de Suscriptores. [35]	Nuevas funciones de Seguridad: • Tráfico del Plano de Usuario Exclusivo. • Control de vivienda aumentada. • Privacidad del suscriptor. • Estructura de Autenticación Unificada. • Proxy de protección. [35]
Protocolos	Protocolos rezagados en el Plano de Control LTE. [30]	Utiliza PDPC en la Capa 2 para: • Cifrado y descifrado basado en el estándar de cifrado avanzado AES. [página 116] • Cifrado del Plano de Usuario y de la Integridad. [página 116]
• Implementación de SDN [30] • NFV [42]		Seguridad por niveles; a un Segmento o recurso. [40] Inclusive una Gestión de Seguridad unificado. [40]

		Diferentes requisitos de Red y Seguridad para cada servicio. [40]
Orquestación	Operaciones de Seguridad difíciles de escalar, limitando la utilización de aplicaciones exclusivas. [40]	• Orquestación Automática e instalación remota. [42] A través de Políticas de Seguridad programables para garantizar una Red confiable y segura que cumpla con los requerimientos de nivel de servicio. [40]
Arquitectura	Arquitectura generacional basado en generaciones antiguas. [18]	• Mejora en la privacidad en la reorganización de una Arquitectura de Red más distribuida y basada en servicios. [30][40][42] • Separación entre el Plano de Usuario y de Control. [42] [página 96]
Núcleo	Núcleo de Paquete Evolucionado 4G (EPC) [40]	Evolución Núcleo 5G [40] • Entorno de Nube de Telecomunicaciones Distribuido con Funciones de Red Física (PNF). [40]

2.7.4 Semejanzas entre servicios brindados de Seguridad en Redes Inalámbricas de ambas generaciones móviles

Tabla 67 Diferencias entre servicios brindados de Seguridad en Redes Inalámbricas, 4G y 5G. Fuente: Elaboración propia basado en: [18][20]

Semejanzas	4G	5G
IPSec	"IPSec es el protocolo de Seguridad más utilizado para proteger los canales de comunicación en las Redes de Telecomunicaciones actuales." [20]	Nuevas arquitecturas de comunicación basadas en IPSec, para asegurar los Canales de Control y datos 5G. [20]
Monitoreo de Seguridad	Inspeccionar el tráfico de datos desde UE a la CN LTE. [20]	Inspeccionar el tráfico de datos. [20] desde UE a la CN 5G. [20]
Algoritmo de cifrado 128-NEA1	Algoritmo basado en SNOW 3G de 128 bits como se hace referencia en 3GPP TS. [18]	Incluye si es NSA.
Algoritmo de protección de Integridad 128-NIA1	Algoritmo de Protección de Integridad basado en SNOW 3G de 128 bits como se hace referencia en 3GPP TS. [18]	Incluye si es NSA.

Conclusiones

La Red 5G es la primera Arquitectura de Red Móvil diseñada para admitir múltiples casos de uso, esto quiere decir, que la Telefonía Móvil, solamente es un caso de uso entre una gran variedad de aplicaciones y servicios que ofrece 5G.

Sin embargo, esta gran tecnología, cuenta con diversas vulnerabilidades, entre las más importantes se encuentra la Cadena de Suministro, donde a pesar de contar con un Software de Seguridad confiable, los componentes de proveedores externos debilitan la Seguridad, dificultando el avance de mejoras y una calidad eficiente del servicio en áreas determinadas, por ejemplo un país que únicamente arma sus equipos 5G con elementos extranjeros, desconoce sus vulnerabilidades reales, invierte tiempo de valor buscando los riesgos que pudieran generar a mediano o corto plazo.

Al mismo tiempo cuenta con un amplio grado de Seguridad por niveles, por segmento o recurso en comparación de generaciones anteriores, ya que su capacidad es muy extendida.

Ofrece nuevas funciones de Seguridad mediante nuevos Protocolos, Políticas de Seguridad más amplias, así como diversos procedimientos más avanzados y eficientes, para mantener la CIA de los datos y brindar una de las mejores experiencias a los usuarios en la actualidad.

5G a pesar de ser una nueva tecnología, trae consigo nuevas mejoras sin olvidar que contiene muchos riesgos, debido las amenazas que trae consigo aún son desconocidas, tomando en cuenta, que los hackers de sombrero negro están en constante evolución.

Además, se encuentra en las primeras fases de evolución, por lo tanto, no ha generado su implementación a gran escala como se espera en años posteriores, requiere de muchos

aspectos para poder implementarse en su totalidad como el apoyo del usuario para mudar hacia un Teléfono Móvil compatible y así poner a prueba sus características por encima de 4G.

Con los conocimientos previos que he adquirido en mis materias de la carrera de Ingeniería en Redes, este trabajo de investigación me ha ayudado a comprender con mayor facilidad la estructura, funcionamiento, los riesgos que suponen cada una de ellas, sus aplicaciones en el ámbito doméstico, industrial entre otras, es decir, todo lo que involucra este tema de Seguridad en Redes 5G que es una aplicación de la vida cotidiana.

Comenzando desde lo más simple como es la definición de Telefonía Celular, los elementos que hacen posible su funcionamiento, etc. En esta sección me llamó la atención la organización celular, no tenía intención de agregar esta parte, pero me surgió la necesidad de investigar un poco más y así poder resolver todas mis dudas, que quizás pueden ayudar a otras personas encontrando en un mismo lugar, entender que no se trata solamente de sus componentes, sino que su funcionamiento desde lo más pequeño es muy interesante.

La evolución de los estándares de la telefonía mediante versiones, ofreciendo mejoras cada vez más innovadoras, mejorando la capacidad de comunicación, la incorporación de nuevos sistemas y antenas para la transmisión y recepción de las señales.

La evolución de la telefonía no se encuentra mucha información acerca de la generación 0, antecesora del 1G, comenzando como un equipo muy pesado que solamente podía ser montado a un automóvil para poder usarse, similar a la siguiente generación que fue el 1G, pero sin prestar atención a la seguridad, las escuchas clandestinas comenzaban a surgir como el inicio de un querer obtener un provecho a las vulnerabilidades existentes, si una persona es curiosa, esta recopilación de datos puede ayudar a entender un poco mejor como era cada una de las generaciones incluyendo sus IMT, basándose siempre en conceptos simples desde Telefonía celular para que poco a poco mejore la comprensión, incluyendo la línea de tiempo de generaciones móviles.

Iniciando con el Capítulo 2 el concepto que tenía en mente de la Quinta Generación Móvil no era del todo cierta, ya que es muy diferente a las demás generaciones, 5G lo que comúnmente conocemos no sólo es telefonía, sino una aplicación, un punto en un sinfín de aplicaciones que es el Internet de las Cosas, es por eso, que a veces existe esa confusión

más que nada en América Latina, al no conocer del todo 5G, ya que en otros países ha estado en funcionamiento pero por la pandemia y otros factores no había llegado a México, como tampoco ha evolucionado tanto como 4G ya que depende de esta llamándose 5G no autónomo.

Los requerimientos que ofrece 5G es por un cambio de arquitectura diferente a 4G, aunque cada componente tiene un nombre y una función diferente, con nuevas características, manteniendo los elementos en conjunto como otras generaciones. Realizando una separación entre IoT y 5G básico, ya que también surgen nuevos estándares como Lora, Ingenu.

El declive de Bandas de Frecuencia disponibles y considerando las Frecuencias altas para su utilización continua a pesar de la movilidad de los usuarios, pero preservando las Frecuencias medias y bajas de acuerdo con su aplicación por ejemplo las Frecuencias bajas para la división de Celdas llegando a áreas donde no llega la señal ya sea por una Interferencia de la señal.

Asimismo, los riesgos y seguridad a implementar para mantener segura los datos, manteniendo siempre la Confidencialidad, Disponibilidad, Integridad de los datos, mitigando todos posibles inconvenientes a largo plazo que pudieran surgir.

Este documento es la recopilación de lo esencial para el tema de Seguridad en Redes 5G.

Referencias Bibliográficas

[1] *«CCNA Security.»* Netacad.com Capítulo 1, Capítulo 11.

[2] *«Concepto de Firewall.»* Disponible en https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

[3] Página Web: CIC Consulting Informático (2021) *«Seguridad de la Información y Ciberseguridad ¿Es lo mismo?»* Cantabria, España. Disponible en: https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/

[4] Jon Erickson (2008) *«Hacking: The Art of Exploitation. »* 2ND Edition ISBN-13: 978-1-59327-144-2 ISBN-10: 1-59327-144-1 488 / 492 pages (pp.15 - 20)

[5] Alllen Harper, Regalado D., Linn R., Sims Stephen., Spasojevic Branko, Martinez L., Baucom M., Eagle C., Harris Shon (2018) *«Gray Hat Hacking. The Ethical Hacker´s Handbook»* Fifth Edition by McGraw-Hill Education. 792 pages (pp. 37 - 44)

[6] Instituto de Ingeniería UNAM *«Hackers.»* Disponible en http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/hackers.aspx

[7] Hussain, S.R., Chowdhury, O., Mehnaz, S., & Bertino, E. (2018). «LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. *» NDSS*. Disponible en:

[8] Aditya Gupta (2019) «*The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things.* » Apress. Walnut, CA, USA. ISBN 1-4842-4300-5 320 / 330 pages (pp. 1 – 10, 14 - 52, 228, 231 – 308)

[9] Yu-Kwong Ricky Kwok, K. N. Lau Vicent (2007) *«Wirelesss Internet and Mobile Computing: Interoperability and Performance. »* Colorado State University. ISBN 13 9780471679684 773 pages (pp. 111 - 119)

[10] Herrera Pérez, E. (1998) *«Introducción a las Telecomunicaciones Modernas.»* Disponible en Editorial Limusa, S.A. de C.V. Grupo Noriega Editores. México D.F. ISBN 968-18-5506-X5.1 409 páginas (pp. 24 - 25, 32 - 33)

[11] Stallings William (2006) *«Data and Computer Communications. »* Eighth Edition (pp.415 - 416, 419 - 422, 424 - 426) Editorial Pearson Prentice Hall. Upper Saddle River, New Jersey. USA. ISBN: 0-13-243310-9 8th Edition 901 pages (pp.415 - 416, 419 - 422, 424 - 426)

[12] Cybersecurity and Infraestructure Security Agency (2021) *«5G: The Basics. »* Disponible en: https://www.cisa.gov/sites/default/files/publications/5g_basics_infographic_508.pdf

[13] Wayne Tomasi (2003) *«Sistemas de Comunicaciones Electrónicas.»* Cuarta Edición. Prentice Hall. DeVry Institute of Technology. Phoenix, Arizona. México. ISBN 970-26-0316-1 ISBN 0-13-022125-2 976 páginas (pp. 33, 867 - 878)

[14] Saad Z. Asif (2019) *«5g Mobile Communications: Concepts and Technologies. »* CRC Press. Taylor & Francis Group http://taylorandfrancis.com First edition. Boca Raton, FL. ISBN 9780429466342. LC. Classification: LCC TK5103.2 .A47 2018. DDC 621.3845/6--dc23 335 / 355 pages (pp. 15, 17 - 20, 25, 26, 29, 32, 43 - 51, 60 – 66, 74, 131-135)

[15] Dahlman Erick., Parkvall Stefan., Skôld Johan. (2018) *«5G NR: The Next Generation Wireless Access Technology »* Academic Press. An imprint of Elsevier. ISBN: 978-0-12814323-0. Elsevier, Book Aid International. 469 pages. (Chapter 1 - 2, 4)

[16] TTA A Global Partnership (2021) *«3GPP. The Mobile Broadband Standard »* Disponible en https://www.3gpp.org/specifications/releases

[17] Abu-Rgheff., Mosa Ali (2020) *«5G Physical Layer Technologies. »* IEEE Press Centre for Security Communications and Network Research. University of Plymouth. United Kingdom. Edition First John Wiley & Sons Ltd. Identifiers: ISBN 10 1119525519. 554 /579 pages. (pp. 1 - 10, 25, 46, 79 – 81, 102 - 104)

[18] Jyrki T. J. Pennttinen (2019) *«5G Explained. Security and Deployment of Advanced Mobile Communications. »* Atlanta, Georgia, USA. Edition First. John Wiley & Sons Ltd. NJ. USA. Identifiers: LCCN 2018050276 (print) | LCCN 2018052072 (ebook). ISBN 10 1119275687 337 pages (pp. 2 - 5, 8 – 17, 24 – 29, 32, 34, 35, 37, 38, 47 - 52, 53, 55 – 68, 71 - 91, 97 – 100, 105 – 114, 120 - 132, 136, 141 – 150, 154 – 157, 165 – 168, 173 – 181, 193 – 199, 271 - 274)

[19] Ulrick Trick (2021) *«5G An Introduction to the 5th Generation Mobile Networks. »* DE Gruyter Oldenbourg. Frankfurt University of Applied Sciences M., Germany. ISBN 978-3-11-072437-0 294 pages (pp. 1, 2, 9, 10, 11, 14, 30, 31, 34 – 37, 98 – 118, 120 - 124, 140 – 143, 203 – 206, 209 - 216)

[20] Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) *«A Comprehensive Guide to 5G Security.»* Universidad of Oulu, Finland., VMware Inc. USA. Linkoping University, Sweden. Edition First. John Wley & Sons Ltd. ISBN: 9781119293040 483 pages (pp. 6 - 24, 26, 27, 31 – 36, 38 – 50, 52 - 54, 59 – 72, 77, 78, 81 – 87, 89 – 92, 99 – 103, 119 - 221)

[21] UIT (2018) *«Sentando las bases para el 5G: Oportunidades y desafíos.»* Disponible en: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.5G_01-2018-PDF-S.pdf ISBN *978*-92-61-27583-9 Suiza Ginebra. 44 páginas (pp. 4, 5, 7, 12, 14, 17 - 18, 28 – 33, 129-130)

[22] MinTIC (2019) *«Plan 5G Colombia. El futuro Digital es de todos.»* Disponible en: https://mintic.gov.co/portal/715/articles-118058_plan_5g_2019120.pdf 93 páginas. (Capítulo 1 - Capítulo 4)

[23] Raúl Ibarra, Miguel Serrano López (2007) *«Principios de teoría de las Comunicaciones.»* Editorial Limusa, S.A. de C.V. México. 321 páginas (pp. 8, 9)

[30] Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) *«5G Networks: A Review From the Perspectives of Architecture, Business Models, Cybersecurity»* Disponible en http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S2631-26542021000100006&lng=en&nrm=iso&tlng=en Universidad Sergio Arboleda, Bogota Colombia. (Chapter 1 - 2)

[24] Sassan Ahmadi (2019) *«5G NR Architecture, technology, implementation and Operation of 3GPP New Radio Standars. »* 1St Edition June 15. ISBN: 9780128134023 1028 pages (Chapter 1)

[25] Dirección de Ciencia y Tecnología (2020) *«5G Introduces New Benefits Cybersecurity Risks»* (p.1 - 2)

[26] Cybersecurity and Infraestructure Security Agency (2019) *«Overview of Risks Introduced by 5g Adoption in The United States. »* Disponible en: https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf Critical Infraestructure Security and Resilience Note. 1200 EDT

[27] GSMA (2020) *«La Economía Móvil en América Latina 2020.»* Disponible en https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/12/GSMA_MobileEconomy2020_LATAM_Esp.pdf 42 páginas. United Kingdom. (pp. 2 - 25, 39)

[28] Sony Ericsson (2021) *«Harnessing the 5G Consumer Potential: The Consumer Revenue Opportunity Uncovered. »* Disponible en: www.ericsson.com/consumerlab. Ericsson Consumer and Market Insight Report. (pp. 2, 7 - 8, 10)

[29] Apple Inc. (2021) *«Usar la Red 5G con el IPhone.»* Disponible en ttps://support.apple.com/es-mx/HT211828 México

[30] Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) *«5G Networks: A Review from the Perspectives of Architecture, Business Models, Cybersecurity, and Research Developments. »* 2021, vol.4, n.1, pp.6-41. June 01, 2021. ISSN 2631-2654. https://doi.org/10.37135/ns.01.07.01 Disponible en http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S2631-26542021000100006&lng=en&nrm=iso&tlng=en Universidad Sergio Arboleda, Bogotá Colombia. Universidad Politécnica Salesiana, Cuenca, Ecuador, Facultad de Informática, Universidad Nacional de La Plata, Buenos Aires, Argentina. 36 pages. (Chapter 2 y 3.0, 2.1 - 2.3, 4, 5.2)

[31] Dongfeng Fang, Yi Qian., Rose Qingyang Hu., (2018) *«Security for 5G Mobile Wireless Networks. »* Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8125684 (Chapter 1, Chapter 9) Department of Electrical and Computer Engineering. University of Nebraska Lincoln, Omaha, NE 68182, USA. Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84321, USA. Digital Object Identifier 10.1109/ACCESS.2017.2779146 25 pages (Cap. 1, Cap. 9)

[32] Manish Mandloi, Devendra Gurjar, Prabina Pattanayak, Ha Nguyen (2021) *«5G and Beyond Wireless Systems PHY Layer Perspective.* » Springer Singapore: Series in Wireless Technology. Center for TeleInFrastruktur, C1-107, Aalborg University, Denmark. Department of Electronics and Telecommunication Engineering SVKM´s NMIMS, Shirpur, India. Department of Electrical and Computer Engineering University of Saskatchewan, Saskatoon, SK, Canada. 1st Ed. ISBN 13 9789811563904 425 pages (pp. 1 - 2, 5, 6, 13, 21 - 23, 129 – 134, 341 – 355)

[33] GSMA (2019) *«Espectro 5G Posición de política pública de la GSMA.»* Disponible en https://www.gsma.com/spectrum/wp-content/uploads/2019/10/5G-Spectrum-Positions-SPA.pdf (pp. 1 - 10)

[34] Cisco *«Como mantener segura la Red.»* Disponible en http://itroque.edu.mx/cisco/cisco1/course/module11/11.2.2.2/11.2.2.2.html

[35] Cichonski Jeff (2020) *«5G Standardization, 5G Security Enhancements, and Supporting Infrastructure Security Considerations.»* Information Technology Laboratory (NIST). National Institute of Standards and Technology. U.S. Department of Commerce.

[36] Dropmann Ulrich (2019) *«5G Standardization and Spectrum. From 5G Introduction to Long – Term 5G Evolution. »* WebEx Virtual Event. Head of Standardization. June 6, Nokia Disponible en https://www.nokia.com/industryanalysts/sites/ia/files/2020-08/nokia_5g_virtual_event_june_2019_dr_ulrich_dropmann_final_0.pdf (pp. 3, 5, 7, 11, 14, 15)

[37] Mantas, G., Komninos, N., Rodriguez, J., Logota, E. & Marques, H. (2015) *«Security for 5G Communications. »* In: J. Rodriguez (Ed.), Fundamentals of 5G Mobile Networks. John Wiley & Sons, Ltd. ISBN 9781118867464 (Capítulos 9.3, 9.3.1.2 – 9.3.4)

[38] UIT (2021) *«Grupo de Trabajo 5D.»* Disponible en https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx

[39] Homeland Security (2020) *«5G Introduces New Benefits Cybersecurity Risks. »* Disponible en https://www.dhs.gov/science-and-technology/news/2020/10/15/feature-article-5g-introduces-new-benefits-cybersecurity-risks

[40] Jim Hodges, Chief Analyst (2019) *«5G Security Strategy Considerations. A Heavy Reading Whitepaper Produced for Juniper Networks. »* Juniper Networks. Heavy Reading White paper. Pages 9

[41] UIT-T (2020) *«Rec. X.1372. Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Aplicaciones y Servicios Seguros (2) Seguridad de los Sistemas de Transporte Inteligentes (STI). Directrices de Seguridad para la Comunicación entre el Vehículo y su Entorno (V2X) .»* (pp. 5 – 26)

[42] Carugi, Marco (2018) *«Key Features and Requirements of 5G / IMT - 2020 Networks. »* ITUI-T Q2 / 13 Disponible en: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2018/RDF/Workshop%20Presentations/Session1/5G-%20IMT2020-presentation-Marco-Carugi-final-reduced.pdf ITU Expert. Associate Rapporteur and SG13 Mentor. ITU Arab Forum on Emerging Technologies. Algiers, Algeria.

[43] CISA Cyber-Infraestructure (2021) *«Potential Threat Vectors to 5G Infraestructure. »* Disponible en: https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf

Some objects were designed by Edraw Max & freepik.com

Lista de Acrónimos

1 + D Investigación y Desarrollo

1G Primera Generación de Telefonía Móvil

2G Segunda Generación de Telefonía Móvil

3G Tercera Generación de Telefonía Móvil

3GPP Proyecto de Asociación de Tercera Generación

4G Cuarta Generación de Telefonía Móvil

5G Quinta Generación de Telefonía Móvil

AKA Acuerdo de Autenticación y Clave

AMPS Sistema de Telefonía Avanzado

APT Organismo Regulador y Administrador

ARIB Organismo SDO 3GPP en Japón y TTC

ARP Auto Radio Phone

ATIS Organismo SDO 3GPP en Estados Unidos

BS Estación Base

CCSA Organismo SDO 3GGP en China

CDM Multiplexación por División de Código

CDMA2000 Estándar CDMA

CEPT/ECC Europa Organismo Regulador y Administrador TACS Sistema de Comunicaciones de Acceso Total

CN Red central

CITEL América Organismo Regulador y Administrador

C-RAN RAN en la Nube

DFT Transformada Discreta de Fourier

DL Enlace Descendente

DTLS Datagram Transport Layer Security

EDGE Enhanced Dada Rates for GSM Evolution

eNodeB Nodo B

emBMS Servicios de Multidifusión Multimedia Evolucionadas

EPC Paquete de Núcleo Evolucionado

EPS Sistema de Paquetes Evolucionado

ETACS Total Access Communication System

ETSI Organismo SDO 3GPP en Europa

FDD Duplex por División de Frecuencia Pareado

FMC Convergencia Móvil Fija

FSK Modulación por Desplazamiento de Frecuencia

GFDM Multiplexación por División de Frecuencia Generalizada

GPRS Servicio General de Radio por Paquetes

GSMA Asociación GSM

GSM Sistema Global para Comunicaciones Móviles

HSPA High Speed Packet Access

HSPA+ High Speed Packet Access Avanzado

HSS Servidor Abonado Doméstico

IDS Sistema de Detención de Intrusiones

IEEE-SA Instituto de Ingenieros Eléctricos y Electrónicos

IMT Sistema de Telecomunicaciones Móviles

IMT-2000 Telecomunicaciones Móviles para 3G

IMT-Avanzado Sistema de Telecomunicaciones Móviles para 4G

IoT Internet de las Cosas

IPS Sistema de Prevención de Intrusiones

IS-94 Interim Standard

IS-95 Ejemplo de redes 2G basado en CDMA

ITU-T Sector de Normalización de Telecomunicaciones de la UIT

LRSA Sistema de Seguridad Ligero y Robusto

LTE Long- Term Evolution. Evolución a largo plazo

MAC Capas de Control de Acceso al Medio

M2M Comunicación Máquina a Máquina

MDM Gestión de Dispositivos Móviles

MIMO Entidad de Gestión Móvil de Múltiples Antenas. Multiple Input Multiple output

MME Función de la Entidad de Gestión de Movilidad

MTA Automático Sueco Sistema de Telefonía Móvil versión A

MS Abonado Móvil

MSC Centro de Computación Móvil

N Número

NEF Función de Exposición de Red

NF Función de Red

NFV Virtualización de Funciones de Red

NGC Núcleo de Próxima Generación

NGMN Redes Móviles de Próxima Generación

NMT 450 Telefonía Móvil Nórdica

NMT 9000 Telefonía Móvil Nórdica versión más actualizada en ese entonces

NR Nueva Radio

NSS Subsistema de Conmutación de Red

NVF Virtualización de Funciones de Red

OCDE Organización para la Cooperación y el Desarrollo Económico

P-GW Puerta de Enlace de Red de Paquetes de Datos

PHY Capa Física

RAN Red de Acceso por Radio

RFID Identificación por Radiofrecuencia

RRM Gestión de Recursos de Radio Multicelda

Rx Receptor

SCMA Acceso Múltiple de Código Disperso

SDN Redes Definidas por Software

SDO Organizaciones de Desarrollo de Estándares

S-GW Servidor Gateway

SIDF Función de Eliminación de Ocultamiento de Identificador de Suscripción

SIM Módulo de Identidad del Abonado

SISO Sistema Convencional de Entrada y Salida Única

SUPI Identificador Permanente de Suscripción

SUCI Identificador Oculto del Suscriptor

TACS Sistema de comunicaciones de Acceso Total

TDD Dúplex por División de Frecuencia No Pareado

TDMA Acceso Múltiple por División de Tiempo

TLS Transport Layer Security

TSDSI Organismo SDO 3GPP en India

TTA Organismo SDO 3GPP en Corea

Tx Transmisor

UART Receptor / Transmisor Asíncrono Universal

UE Equipo de Usuario

UFMC Filtro Universal de Multiportadora

UIT Unión Internacional de Telecomunicaciones

UL Enlace Ascendente

UMTS Sistema Universal de Telecomunicaciones Móviles

USSSD Servicio de Datos Suplementarios No Estructurados

UTRAN Red de Acceso de Radio Universal

V2V Comunicación de Vehículo a Vehículo

V2X Comunicación de Vehículo a Cualquier Cosa

WCDMA Sucesor de GSM en Conjunto con CDMA

WiMax Representante de Ruta 3G Avanzada

WiMax-Advance WiMax Avanzado

Glosario

Acceso Asistido por Licencia

"Cuando el operador tiene una licencia exclusiva para un cierto rango de frecuencia para planificar la Red o controlar la situación de interferencia." [15]

Actor malicioso, malintencionados, de sombrero negro, ciberdelincuentes o actores cibernético, Identidad no autorizada, Usuarios no autorizados

"Un agente que emplea una acción basada en una computadora y / o una Red contra un objetivo." [43]

AMF

"Función de gestión de acceso y movilidad [30] admite el cifrado de señales de estrato sin acceso NAS aplicando uno de los nuevos algoritmos de radio NEA de conjunto NEA0, 128-NEA1 y 128-NEA2." [18]

Ancho de Banda

"Ancho de Banda máximo agregado del sistema y puede consistir en una o más portadoras de radiofrecuencia (RF)." [18]

"Máximo agregado del sistema y puede consistir en una o más portadoras de radiofrecuencia (RF)". [18]

Antena

"Es el componente responsable de convertir la información en señales electromagnéticas que pueden viajar a través del medio de propagación." [8] generalmente en el aire si se trata de una comunicación inalámbrica o por medios guiados aquellos que utilizan cable de datos para realizar la comunicación.

AS

"Servidor de Aplicaciones." [19]

Ataque de superficie

“Lugares de una computadora o Red de Telecomunicaciones donde un límite de confianza puede ser cruzado por una persona o Software / Hardware no autorizados.” [43]

Automatización de Seguridad de la Red

“Es el proceso de minimizar la iteracción hombre – máquina delegando funciones de control complejas a las máquinas para mayor confiabilidad y precisión.” [20]

Backhaul

“El primer tramo entre RRU y la Red de Núcleo.” [14]

Basado en servicios

“Se refiere a la capacidad de los elementos de la arquitectura que se constituye como funciones de Red (NF) ofreciendo servicios específicos a través de interfaces a cualquier función de Red que se le permita hacer el uso de estos servicios proporcionados.” [18]

BGCF

“Funcion de control de Puerta de Enlace de ruptura,” [19] decide donde salir de la PSTN si es necesario, recibe la solicitud SIP de CSCF cuando se conecta a una Red de conmutación de circuitos.

BSC

“Controlador de la Estación Base.” [19]

Canales Físicos

Canales Físicos de Enlace Ascendente

“Es un conjunto de elementos de recursos que transportan la información que se origina en capas superiores. Los canales Físicos 5G definidos por 3GPP son:

- Canal Compartido de Enlace Ascendente Físico (PUSCH)
- Canal de Control de Enlace Ascendete Físico (PUCCH)
- Canal Físico de Acceso Aleatorio (PRACH).

Canales Físicos de Enlace Descendente

“Se refiere a un conjunto de elementos de recursos que transportan información procedente a capas superiores. 3GPP para 5G define los siguientes canales Físicos de Enlace Descendente:

- Canal Compartido de Enlace Descendente Físico (PDSCH)
- Canal de Transmisión Físico (PBCH)
- Canal de Control de Enlace Descendente Físico (PDCCH).

” [18]

Capacidad del Canal

“Se define como su velocidad de datos máxima alcanzable.” [32]

Capacidad del Tráfico del Área

“Es el rendimiento total del tráfico dentro de un área geográfica determinada y se expresa en Mb/s/m.2.” [18]

Celdas pequeñas

“División de Célula” [18]

Compartir espectro

“Se espera que el espectro se comparta entre usuarios primarios y secundarios cognitivos en redes 5G.” [14]

Comunicación dispositivo a dispositivo

“Entre sistemas celulares utilizando una estación base y el MCS para la comunicación.” [15]

Comunicación dual

“Dispositivo conectado simultáneamente en dos celdas.” [15]

Comunicación tipo máquina

“Todos los tipos de comunicación entre máquinas.” [15]

Compartir espectro

“Uso colectivo de una Banda de Frecuencias de dos o más partes en un área geográfica específica.” [14]

Computación en la nube

“Se ha considerado como una solución ideal para rediseñar la arquitectura RAN actual. Las funciones de la Red Central se realizan como máquinas virtuales o contenedores controlados por el administrador de la nube.” [20]

Conectividad dual

“Situación cuando una computadora está conectada a dos Celdas.” [30]

CSCF

“Función de control de sesión de llamada.” [19] consulta el HSS durante el registro para el S-CSF responsable que funciona como un servidor proxy SIP.

Densidad de Conexión

“Es el número de dispositivos 5G que se pueden cumplir con el nivel de calidad de servicio objetivo dentro de un área geográfica.” [18]

Densificación, Células pequeñas y despliegues Heterogéneos

“Como medio para proporcionar una capacidad y velocidades de datos muy altas.” [15]

Densificación de la Red

“Implica agregar más sitios celulares para aumentar la capacidad de la Red disponible” [17]

Detención del espectro

“Implica sondear el espectro, capturar la información y localizar una parte no utilizada para compartir.” [14]

Dimensiones de Seguridad según la UIT-T

“Control de Acceso, Autenticación, No repudio, Confidencialidad, Seguridad en la Comunicación, Integridad de los Datos y Disponibilidad.” [22]

Disponibilidad

"Es el grado en que un servicio es accesible y utilizable por cualquier usuario legítimo cuando y donde se solicita." [31]

DTLS

"Se utiliza para proteger los datos entre aplicaciones que se comunican, principalmente el tráfico UDP." [20]

Eficiencia Energética

"Indica la capacidad de la tecnología de interfaz de radio (RIT) y el conjunto de RIT (SRIT) para minimizar el consumo de energía de la Red de Acceso por Radio (RAN)." [18]

Eficiencia Espectral Máximo

"Se mide en bits/s/Hz normaliza la velocidad máxima de datos de una única estación móvil en las mismas condiciones ideales sobre el Ancho de Banda del canal utilizado.[18] La Eficiencia Espectral Máxima para el enlace descendente se establece en 30 b/s/Hz mientras el ascendente en 15 b/s/Hz para 5G." [18]

Eficiencia Espectral Promedio

"También llamado "Eficiencia del Espectro." Es el rendimiento agregado y se calcula a través de los bits SDU recibidos correctamente de la capa 3." [18]

EIR

"Registro de identificación de equipos." [19]

Escuchas clandestinas

"Es un ataque que utiliza un receptor no intencionado para interceptar el mensaje de otros." [31]

Estándares IEEE

"IEEE 802.22 Para redes de Área Regional Inalámbricas (WRAN)

IEEE 802.11af para Redes de Área Local Inalámbricas (WLAN)

IEEE 802.19.1 para la coexistencia

IEEE 1900 para Redes y Sistemas de Radio de Acceso Dinámico al Espectro.” [14]

Fiabilidad

“Es la capacidad del sistema para entregar la cantidad deseada de paquetes de datos en las capas 2 y 3.” [18]

Fronthaul

“Es el enlace entre un grupo de Unidades de Banda Base y Unidades de Radio Remotas (RRU) que colectivamente formaron el concepto de C-RAN” [14]

Ganancia

“Es la relación entre la potencia de salida y la potencia de entrada. Una ganancia mayor que 1 donde la potencia de salida es mayor que la potencia de entrada se llama amplificación.” [8]

GFDM

“Es uno de los métodos de transmisión de múltiples portadoras no ortogonales que se ha considerado para los sistemas 5G.” [14]

GGSN

“Nodo de soporte GPRS de Puerta de Enlace.” [19]

GMSC

“Centro de conmutación móvil del Gateway.” [19]

gNB

“Estación basada en 5G. Sirve para los dispositivos NR que utilizan los protocolos del Plano de Usuario y de Control NR.” [30]

Helnet

“Es una técnica que proporciona una cobertura inalámbrica general y un alto rendimiento en Redes Inalámbricas 5G.” [31]

HLR

"Registro de Ubicación de Origen." [19]

HLR AuC

"Registro de ubicación de origen con autenticación." [19]

HSS

"Servidor Abonado Doméstico." [19]

IBCF

"Funcion de control de fronteras de interconexión." [18]

Interfaz aérea

"Enlace entre el usuario / dispositivo inalámbrico y la Unidad de Radio Remota." [30][14][18]

ISDN

"Redes digitales de servicios integrados." [20]

Latencia

"En el Plano del Usuario se refiere al tiempo que tarda la fuente en enviar un paquete en la capa de Protocolo de Radio 2/3 para llegar a su destino en la capa respectiva y se expresa en milisegundos." [18]

"Retraso en la transmisión y procesamiento de los datos, como el retraso entre el envío de un comando y su ejecución."

Límite de confianza

"Límites por lo cual agentes de diferentes organizaciones o los niveles de confianza interactúan." [43]

MGCF

"Funcion de control de puerta de enlace multimedia." [19]

MGW

“Puerta de enlace de medios.” [19]

MIMO

“Es una tecnología de antena para comunicaciones inalámbricas en la que se utilizan múltiples antenas para transmitir y recibir datos.” [20] Varios usuarios son atendidos simultáneamente por una estación base de múltiples antenas.

“El utilizar un mayor número de antenas resuelve el problema de rendimiento en la Red, la cobertura y la velocidad de datos limitados.” [32]

MRFC

“Controlador de Funciones de Recursos Multimedia.” [19] Para el control de procesamiento de los datos de los usuarios.

MRFP

“Se usa para el manejo de dato de usuario en el IMS como grabación y reproducción de voz.” [19]

MSC / VLR VLR

“Registro de ubicación de visitantes.” [19]

Movilidad

“Velocidad máxima de la Estación Móvil de tal manera que se siga cumpliendo el requisito mínimo de QoS.” [18]

Movilidad del espectro

“La necesidad de la movilidad del espectro surge cuando las condiciones actuales del canal empeoran para los usuarios de CR o aparece una PCU en el área.” [14]

ng-eNB

“Para servicios LTE utilizando protocolos de Plano de Control y usuario LTE.” [30]

NEF

“Función de Exposición de la Red [30] proporciona exposición externa de las capacidades de la Función de Red (NF) a la Función de Aplicación (AF).” [18]

NFV

“Virtualización de Funciones de Red. Reemplaza la información de la Red en dispositivos específicos tales como cortafuegos, con instancias virtualizadas que se pueden ejecutar en soportes físicos… reduciendo costes de modificaciones y actualizaciones en la Red.” [21]

NOMA

“Esquema No Ortogonal que se usa para mejorar la Eficiencia Espectral.” [14]

NS

“Es un conjunto de características y funcionalidades de servicios a un conjunto de Equipos de Usuario (UE).” [15]

Nuevos escenarios

“Nuevas características de mejorar.” [15]

OFDM

“Es la tecnología que divide una Banda de Frecuencia amplia en varias frecuencias estrechas, subportadoras que transportan los datos reales entre el transmisor y el receptor.” [18]

“Técnica de modulación multiportadora, parte integral de muchos estándares de telecomunicaciones/radiodifusión y su forma CP-OFDM se usa actualmente en LTE, WiMax y LTE Advance.” [14]

Orquestación y Gestión de Redes

“Configuración, gestión de gran cantidad de aplicaciones, recursos físicos y lógicos.” [42]

PCRFa

“Política y Función de Reglas de Carga.” [19]

PCU

“Unidad de Controlador de Paquetes.” [20]

P-GW

“Puerta de enlace de Red de paquetes de datos [20] “controla los servicios de datos IP incluido el enrutamiento, asignación de direcciones IP, aplicaciones de políticas y proporcionar acceso que no es 3GPP.” [20]

PSTN

“Red pública conmutada.” [20]

Radio cognitivo

“Es una posible solución para aumentar la eficacia del espectro asignado infrautilizado.” [14]

RAN

“Es la tecnología clave para que los operadores brinden servicios de alta calidad y velocidad de datos que están disponibles para los usuarios suscritos en cualquier momento.” [17]

Rebanado de Red / Corte de Red

“También llamado Segmentación de la Red.” [14]

Red principal

“Arquitectura basada en servicios e interconectividad de extremo a extremo.” [18]

Redes Definidas por Software

“O bien llamado SDN, es una arquitectura para configurar automáticamente rutas a través de una Red, utilizando principalmente un controlador de SDN.” [43]

Retransmisión

“Implica que el dispositivo se comunica con la Red a través de un nodo de retransmisión, es decir, conectado de forma inalámbrica a una Célula utilizando una Interfaz de Radio.” [15]

RNC

“Elemento de la RAN responsable de controlar el eNB que está conectado a él. La responsabilidad del RNC incluye la gestión de recursos radioeléctricos; algunas funciones de la gestión de la movilidad; y es el elemento donde se realiza el cifrado de datos antes de la transmisión de datos.” [17]

SCMA

“Es una técnica de acceso múltiple basada en un libro de códigos no ortogonal en desarrollo.” [14]

SDN

“Permite la reconfiguración dinámica de los elementos en tiempo real y el control de las Redes 5G.” [21]

SGSN

“Nodo de compatibilidad con GRPS.” [19]

Segmento de Red

“Es una Red lógica que conforme a las necesidades de una empresa o un cliente se configura para dar servicio a la Banda Ancha Móvil, aplicaciones con el mayor soporte de la movilidad, cercano a lo que ofrece LTE.” [30]

Segmentación de la Red

“Permite dividir la Red Física en múltiples redes virtuales llamados “Segmentos,” capaces de soportar diferentes RAN o tipos de servicios… reduciendo costes de construcción de la Red” [21]

“Proporciona los medios para utilizar de forma controlada el conjunto necesario de funcionalidades y servicios PLMN para que los recursos de Red se puedan optimizar por caso de uso.” [18]

SIDF

"Función de eliminación de ocultamiento de identificador de suscripción, es resolver el SUPI (Identificador permanente de suscripción) desde el SUCI (Identificador oculto del suscriptor)." [18]

SLF

"Base de datos, ofrece al AS por ejemplo la posibilidad de terminar la dirección del HSS responsable de un usuario en específico." [19] Función de Localización de Suscriptores." [19]

Stuxnet

"SCADA, lanza ataques críticas a la infraestructura de Red 5G, dañando los servicios." [20]

UFMC

"Es una modificación de la conocida onda CP-OFDM." [14]

Unidad de Banda Base

"En la Unidad de Banda Base, normalmente se lleva a cabo el siguiente procesamiento de señales: filtrado, modulación, / demodulación, procesamiento de predistorsión, detención de señales, estimación de canales, ecualización y codificación /decodificación de señales." [17]

Velocidad Pico de Datos

"Máxima velocidad de datos posible." [18]

TDD Dinámico

"División estática de recursos para mantener múltiples usuarios y carga agregada por celda en el Enlace Ascendente y Descendente para mayor cobertura." [15]

TLS

"Se utiliza para proporcionar privacidad e Integridad de Datos entre usuarios y dispositivos." [20]

Transceptor

“El transceptor consta de un transmisor y un receptor para las comunicaciones UL y DL.” [17]

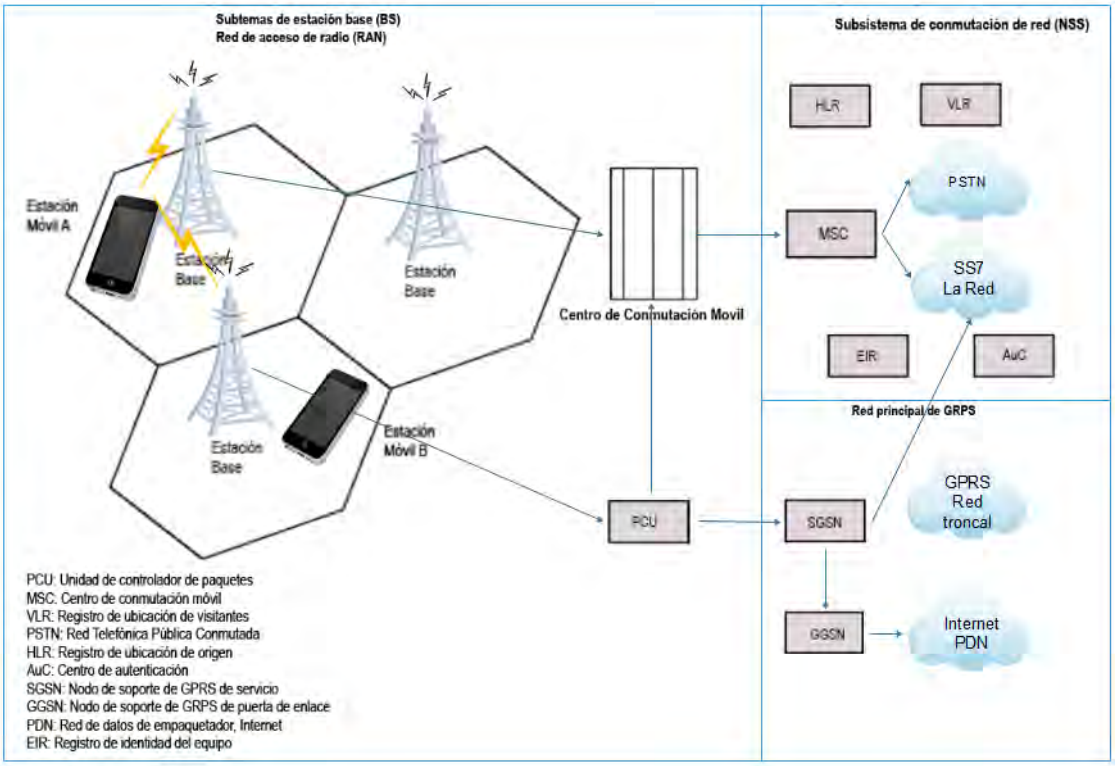
Zonas de confianza

“División de la Red en límites o zonas de confianza. Los datos transferidos entre zonas de confianza se manejan según los principios de la arquitectura básica en servicios del 5G.” [18]

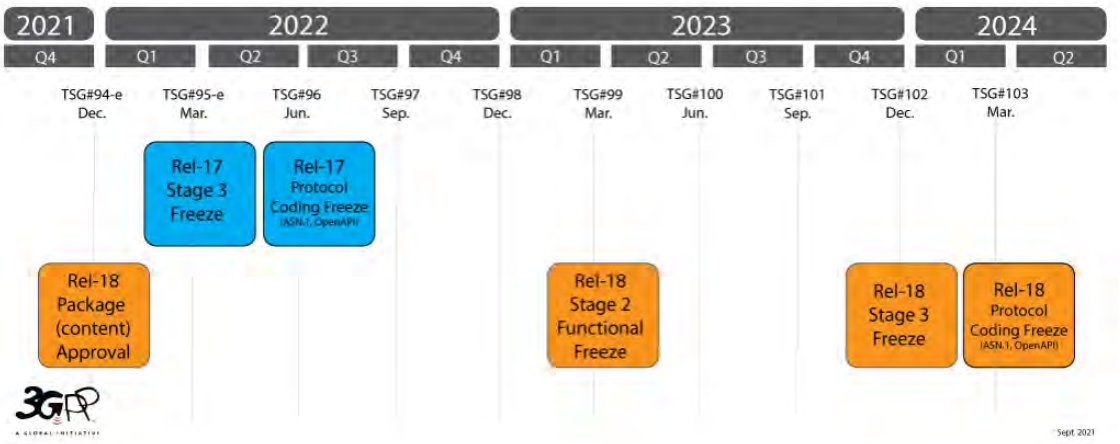
Anexos

El medio de transmisión que utiliza el teléfono Móvil es no guiado porque la comunicación es a través de radiofrecuencia.

Arquitectura de Red GSM. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018)



Lanzamientos 3GPP hasta Ralease 18 y la Fase 3 próximo a partir del 2023. Fuente: TTA A Global Partnership (2021) [16]



Banco de pruebas actuales. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

Banco de pruebas	Localización	Frecuencias [GHz]	Caso de uso
Universidad de Bristol (5GINFIRE, 2021)	Inglaterra	3,5, 26	Seguridad Smarty City
Universidad de Surrey (Universidad de Surrey, 2021)	Inglaterra	2.6, 3.5, 26	Satélite
5G-VINNI (Ghassemian, Muschamp y Warren, 2020; 5G-PPP, 2021)	Inglaterra	3.6, 2.6	Industria (Remoto robótico control, aplicación inmersiva basada en realidad virtual), juegos basados en la nube, medios, e-Health (atención conectada), protección pública y ayuda en caso de desastres
Laboratorio 5G (5G Industrielles Internet, 2021)	Alemania	3,75, 26, 60	Aplicaciones de la Industria 4.0, Hombre-Máquina colaboración, autónoma conducción, asistido por robot telecirugía
5G-EVE (5G Industrielles Internet, 2021)	Grecia, Italia, Francia	3,5, 3,6, 3,8	Aplicaciones de la industria 4.0, ciudades inteligentes, campus inteligente, transporte inteligente
COSMOS (GRUPO COSMOS, 2021)	Estados Unidos	sub-6, 28	Ciudad inteligente

Componentes principales 5G. Elaboración propia basado en:
[9][12][14][15][17][18][19][20][21][22][30][31][32][33][35[36]

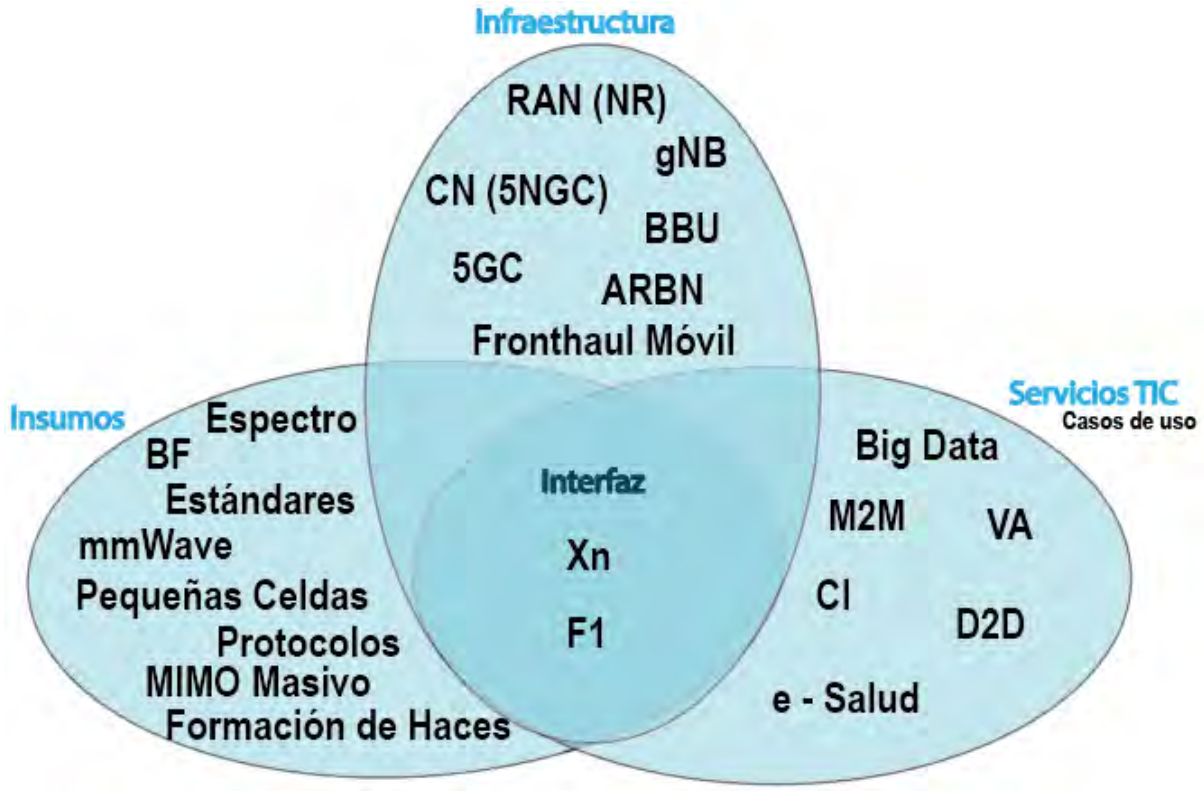
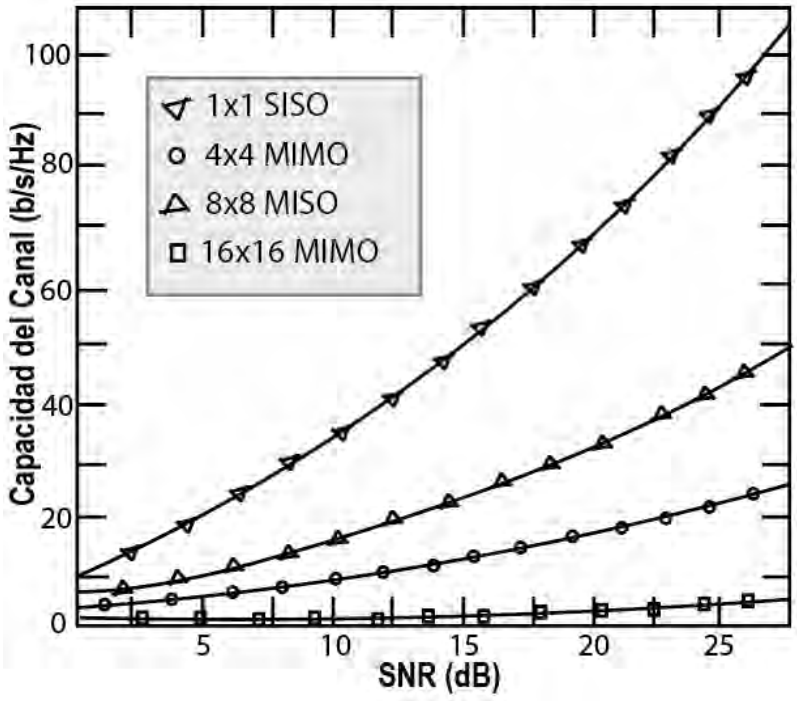


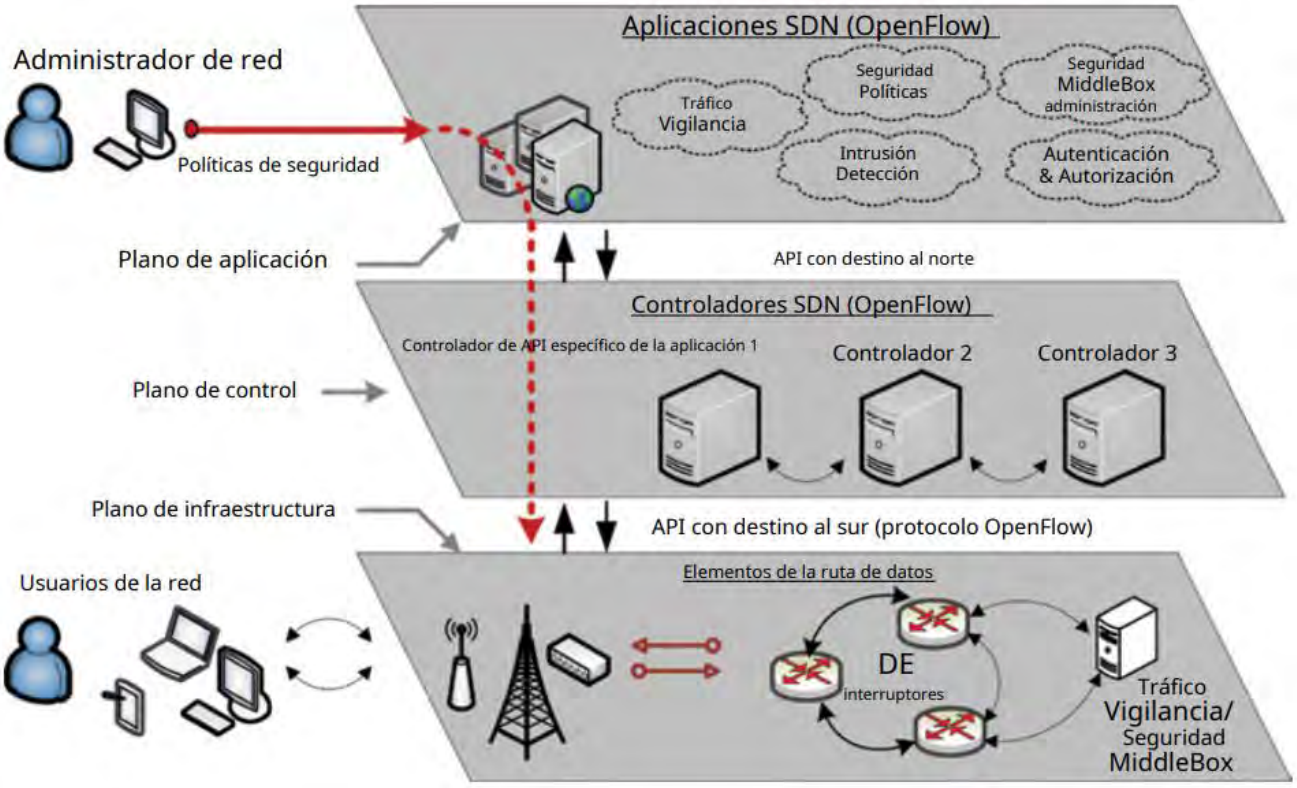
Figura Capacidad del Canal para varios sistemas: (i) 1x1 SISO (ii) 4x4 MIMO (iii) 8x8 MISO (iv) 16x16 MIMO. Fuente: Manish Mandloi, Devendra Gurjar, Prabina Pattanayak, Ha Nguyen (2021) [32]



"En la Figura muestra la comparación gráfica de los sistemas de antenas SISO y MIMO sobre la base de la capacidad del canal y el valor de SNR." [32]

Logos de organizaciones de estandarización. Fuente: TTA A Global Partnership (2021) [16]

Descripción general de la Arquitectura SDN. Fuente: Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, (2018) [20]



Comparación de los KPI Y las características de las Redes 5G y 6G. Fuente: Aranda J., Sacoto-Cabrera E., Haro D., Astudillo F. (2021) [30]

KPI / Funciones	5G	6G
Ancho de banda operativo	Hasta 400 MHz (sub-6 Ghz bandas), hasta 3,25 GHz (bandas mmWave)	Hasta 400 MHz (bandas sub-6 Ghz), hasta 3,25 GHz (bandas mmWave)
Frecuencia máxima	90 GHz	10 THz
Velocidad máxima de datos	35,46 Gbps	1 Tbps
Latencia de los planos de control y usuario	1 ms (uRLLC), 20 ms	25 μs (táctil aplicaciones), 20 ms
Movilidad	500 kilómetros por hora	1000 kilómetros por hora
Arquitectura	MIMO masivo	Superficie inteligente
Redes centrales	Internet, Internet de las cosas	Internet de todo
Multiplexación	OFDMA	OFDMA inteligente
Nivel de servicio	3D VR / AR	Táctil

Requisitos de Seguridad de EU 5G, según la interpretación de 3GPP TS 33.501. Fuente: Jyrki T. J. Pennttinen (2019) [18]

Requisito	Descripción del requisito
Datos de usuario y datos de señalización *confidencialidad*	Para los datos del usuario y la confidencialidad de los datos de señalización, se aplica lo siguiente: 1. El gNB admite el cifrado de datos de usuario y la señalización RRC en UE – gNB. 2. La función de gestión de sesiones (SMF) dicta el uso y el gNB activa el cifrado de los datos del usuario. 3. El gNB admite los algoritmos de cifrado NEA0, 128-NEA1 y 128-NEA2 y, opcionalmente, el 128-NEA3. 4. Es opcional admitir la protección de la confidencialidad de los datos del usuario y la señalización RRC en UE – gNB. Cabe señalar que se insta a que se aplique la protección de la confidencialidad cuando las reglamentaciones lo permitan.
Datos de usuario y datos de señalización *integridad*	Para el usuario y la integridad de los datos de señalización, se aplica lo siguiente: 1. El gNB admite la protección de la integridad y reproduce la protección de los datos del usuario y la señalización RRC en UE – gNB. 2. SMF dicta y gNB activa la protección de integridad de los datos del usuario. 3. El gNB admite algoritmos de protección de integridad NIA0, 128-NIA1 y 128-NIA2 y, opcionalmente, 128-NIA3. No obstante, el uso real de la protección de la integridad de los datos del usuario en UE – gNB se deja como opcional. 4. Los mensajes de señalización RRC, excepto los casos detallados en 3GPP TS 38.331, están protegidos por integridad. La habilitación de NIA0 en gNB depende de los requisitos reglamentarios para el soporte de sesiones de emergencia no autenticadas.
Configuración de gNB y configuración	Para la instalación y configuración de gNB, se aplica lo siguiente: 1. Cuando O&M instala y configura gNB, si el MNO así lo dicta, el gNB autentica y autoriza el procedimiento de acuerdo con el escenario de certificación detallado en 3GPP TS 33.310. Esto es para evitar que las partes externas modifiquen los ajustes y la configuración de gNB mediante el acceso local o remoto. 2. La comunicación en O & M – gNB está protegida por confidencialidad, integridad y reproducción. Las asociaciones de seguridad entre O&M, gNB y la red central 5G se detallan en 3GPP TS 33.210 y TS 33.310. 3. El gNB puede autorizar las intenciones de cambios de software y datos (autorizados). 4. Se aplica un entorno seguro para la ejecución de partes sensibles del arranque. 5. Es necesario garantizar la confidencialidad e integridad del software, que se transfiere a gNB, y la actualización del software de gNB debe verificarse en el momento de la instalación como se indica en 3GPP TS 33.117.
tecla gNB administración	Para la gestión de claves en el gNB, se aplica lo siguiente: 1. La protección de claves es de suma importancia cuando la red central 5G proporciona el material de claves para los gNB. 2. Las partes de la implementación de gNB que almacenan o procesan las claves en formato claro deben estar protegidas de ataques físicos, posiblemente aplicando un entorno físico seguro. Las claves en dicho entorno seguro deben almacenarse solo allí, excluyendo los casos permitidos por las especificaciones 3GPP.
Manejo de usuario y control de datos para el gNB	Para manejar los datos del plano de control y del usuario de gNB, se aplica lo siguiente: 1. Las partes de gNB que almacenan o procesan datos del plano de control o del usuario en formato claro deben protegerse contra ataques físicos. De lo contrario, la entidad debe colocarse en una ubicación físicamente segura para almacenar y procesar los datos del plano de control y del usuario en un formato claro.

Continuación

Requisito	Descripción del requisito
Seguro ambiente de el gNB	El entorno seguro protege la información y las operaciones confidenciales del acceso o la exposición no autorizados. Para el entorno seguro definido lógicamente dentro de gNB, se aplica lo siguiente: 1. Es compatible con el almacenamiento seguro de datos confidenciales y la ejecución de funciones confidenciales como el cifrado y descifrado de datos del usuario. 2. También admite la ejecución de partes sensibles del proceso de arranque. 3. Debe garantizarse la integridad del entorno seguro. 4. Se debe autorizar el acceso al entorno seguro.
gNB *F1* interfaces	El conjunto de NB con implementaciones divididas DU-CU (unidad distribuida, unidad centralizada) basadas en *F1* La interfaz se define en 3GPP TS 38.470. Para el gNB*F1* interfaz, se aplica lo siguiente: 1. Tráfico de señalización F1-C como se define en 3GPP TS 38.470, portador de señalización F1-C como se define en TS 38.472, y los datos del plano de usuario pueden utilizar *F1* interfaz en DU – CU. 2. gNB admite confidencialidad, integridad y protección de reproducción para el portador de señalización F1-C, y el tráfico de administración en la interfaz F1-C (según 3GPP TS 38.470) debe estar protegido por integridad, confidencialidad y reproducción. 3. El gNB admite confidencialidad, integridad y protección de reproducción en la interfaz gNB DU – CU F1-U para el plano de usuario.
gNB E1 interfaces	El 3GPP TR 38.806 describe el *E1* interfaz. Para el gNB*E1* interfaz, se aplica lo siguiente: 1. El 3GPP TS 38.460 define los principios para los gNB con implementación dividida DU-CU, incluida la interfaz abierta entre CU-CP y CU-UP utilizando el *E1* interfaz. 2. La interfaz E1 entre CU – CP y CU – UP está protegida por confidencialidad, integridad y reproducción.