UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DISEÑO DE UNA ARQUITECTURA DE RED UTILIZANDO ISO/IEC 27033 PARA UN SISTEMA DE BUSES INTELIGENTES EN LA CIUDAD DE MACHALA.

GRANDA PALADINES GEORGE JOSHUA
INGENIERO DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

DISEÑO DE UNA ARQUITECTURA DE RED UTILIZANDO ISO/IEC 27033 PARA UN SISTEMA DE BUSES INTELIGENTES EN LA CIUDAD DE MACHALA.

GRANDA PALADINES GEORGE JOSHUA
INGENIERO DE SISTEMAS

MACHALA
2021

UTMACH

FACULTAD DE INGENIERÍA CIVIL

CARRERA DE INGENIERÍA DE SISTEMAS

TRABAJO TITULACIÓN
PROPUESTAS TECNOLÓGICAS

DISEÑO DE UNA ARQUITECTURA DE RED UTILIZANDO ISO/IEC 27033 PARA UN SISTEMA DE BUSES INTELIGENTES EN LA CIUDAD DE MACHALA.

GRANDA PALADINES GEORGE JOSHUA
INGENIERO DE SISTEMAS

LOJA MORA NANCY MAGALY

MACHALA, 27 DE ABRIL DE 2021

MACHALA
2021

Sin título

INFORME DE ORIGINALIDAD

8%	6%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	docplayer.es Fuente de Internet	1%
2	Diego Gutierrez, Francisco Gimenez, Carlos Zerbini, Guillermo Riva. "Measurement of 4G LTE Cells with SDR Technology", IEEE Latin America Transactions, 2020 Publicación	1%
3	Submitted to Universidad Catolica De Cuenca Trabajo del estudiante	<1%
4	Submitted to Universidad Estatal a Distancia Trabajo del estudiante	<1%
5	www.coursehero.com Fuente de Internet	<1%
6	discriminaciongeneraltipos.blogspot.com Fuente de Internet	<1%
7	dof.gob.mx Fuente de Internet	<1%
8	Submitted to Universidad Tecnológica Israel Trabajo del estudiante	<1%

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

El que suscribe, GRANDA PALADINES GEORGE JOSHUA, en calidad de autor del siguiente trabajo escrito titulado DISEÑO DE UNA ARQUITECTURA DE RED UTILIZANDO ISO/IEC 27033 PARA UN SISTEMA DE BUSES INTELIGENTES EN LA CIUDAD DE MACHALA., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

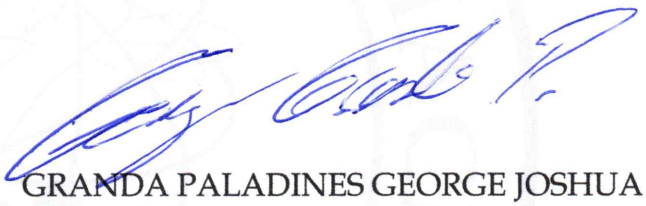
El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

El autor como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 27 de abril de 2021



GRANDA PALADINES GEORGE JOSHUA
0706569597

DEDICATORIA

Con mucho orgullo quiero dedicar mi tesis a mi familia, en especial a mis padres, quienes han sido los pilares fundamentales en todo mi trayecto universitario.

AGRADECIMIENTO

A mi familia por estar siempre presentes en los momentos más importantes de mi vida, por ser mi mayor inspiración y motivación.

De manera especial quiero agradecer a mi tutora de tesis, por haberme brindado sus sabios consejos durante el desarrollo de mi proyecto de titulación, también a los docentes que formaron parte de mi vida académica y finalmente a mis compañeros de clase, quienes supieron brindarme siempre su apoyo.

RESUMEN

En la actualidad la mayoría de los ciudadanos utilizan dispositivos inteligentes con conexión a internet ya sea para el estudio, para el trabajo, o para fines sociales; este tipo de medio se ha convertido indispensable en la vida diaria de cientos miles de personas que requieren estar conectados siempre a toda hora y en todo lugar. Entonces se considera la necesidad de que las personas puedan conectarse a una red confiable y segura, por lo cual se pretende diseñar una arquitectura de red mediante la ISO/IEC 27033 para un sistema de buses inteligentes en la ciudad de Machala, mediante el análisis geográfico de la ciudad, para determinar las rutas de autobuses urbanos que circulan; también se identifican los puntos más remotos a los que llega el autobus con el fin de establecer la ubicación de las antenas enodoB y con ello lograr q la señal de internet no sea interrumpida.

Para la implementación de esta propuesta primero se realizó una investigación de las rutas de los buses urbanos con los que cuenta la ciudad de Machala, los datos precisos fueron recolectados desde la página de Movilidad Machala EP, en donde se pudo constatar que gran número de buses circula por el centro de la ciudad, lo que se supone que existirá un mayor número de antenas concentradas en esta zona, precisamente para recolectar información sobre la cantidad de antenas existentes se indagó en fuentes bibliográficas en la web, además de la aplicación móvil OpenSignal, la cual proporciona información independiente sobre la conectividad móvil a nivel mundial; indicando la disposición de antenas distribuidas por la ciudad y se confirma que los sitios rurales de la ciudad cuentan con menos privilegios en comparación con la zona céntrica, existen menos antenas por ende se asume que la señal de internet se perdería por existir menos antenas además de encontrarse en medio de plantaciones de banano y otros factores que imposibilitan la conexión.

A partir de este análisis geográfico sobre las rutas se efectuó el siguiente análisis para definir la operadora móvil con la que se trabajará, para ello se investigó estadística de los últimos años con respecto a la frecuencia de datos, usuarios y antenas con las que cuentan las operadoras de la ciudad de Machala, con el fin de conocer cuál era la operadora de telefonía móvil más idónea para la implementación de este trabajo, llegando así a reconocer a la operadora Claro

como la operadora con mayor participación en el mercado del Ecuador, teniendo más accesos prepago y pospago, además, se constató mediante la aplicación OpenSignal, que dicha operadora cuenta con un mayor número de antenas ubicadas en el centro de la urbe, por lo que la adquisición de nuevas antenas será en menor volumen.

Luego de estos análisis se procede con el diseño de red en base a la norma ISO/IEC 27033 la cual define los lineamientos a seguir para que la red sea segura y mitigar los posibles riesgos que se presenten durante la conexión de los usuarios. Finalmente se realiza una evaluación a la red mediante una matriz de riesgos por colores dando como resultados los controles o medidas a tomar en consideración para obtener una red más segura y menos propensas a fallos, errores o irrupción de activos.

Palabras clave: arquitectura de red, arquitectura LTE, buses inteligentes, Internet de las Cosas, ISO/IEC 27033

ABSTRACT

Currently, most citizens use smart devices with an internet connection either for study, for work, or for social purposes; this type of medium has become indispensable in the daily lives of hundreds of miles of people who must always be connected at all times and in all places. Then the need for people to connect to a reliable and secure network is considered, for which it is intended to design a network architecture through ISO / IEC 27033 for an intelligent bus system in the city of Machala, through geographic analysis. of the city, to determine the routes of urban buses that circulate; The most remote points to which the bus arrives are also identified in order to establish the location of the antennas enodoB and thereby achieve that the internet signal is not interrupted.

For the implementation of this proposal, an investigation was first carried out of the routes of the urban buses that the city of Machala has, the precise data was collected from the Mobility Machala EP page, where it was found that a large number of buses circulate through the city center, which is supposed to be a greater number of antennas concentrated in this area, precisely to collect information on the number of existing antennas, bibliographic sources on the web were investigated, in addition to the OpenSignal mobile application, which provides independent information on mobile connectivity worldwide; indicating the disposition of antennas distributed by the city and it is confirmed that the rural places of the city have fewer privileges compared to the downtown area, there are fewer antennas, therefore it is assumed that the internet signal would be lost because there are fewer antennas in addition to being in the middle of banana plantations and other factors that make connection impossible.

From this geographical analysis on the routes, the following analysis was carried out to define the mobile operator with which it will work, for this purpose, statistics from recent years were investigated with respect to the frequency of data, users and antennas with which the operators of the city of Machala, in order to know which was the most suitable mobile phone operator for the implementation of this work, thus coming to recognize the Claro operator as the operator with the largest participation in the Ecuadorian market, having more Prepaid and post-paid accesses, in addition, it was verified through the OpenSignal application, that said

operator has a greater number of antennas located in the center of the city, so the acquisition of new antennas will be in lower volume.

After these analyzes, we proceed with the network design based on the ISO / IEC 27033 standard, which defines the guidelines to be followed so that the network is secure and mitigate the possible risks that may arise during the connection of users. Finally, an evaluation of the network is carried out using a matrix of risks by colors, giving as results the controls or measures to be taken into consideration in order to obtain a more secure network and less prone to failures, errors or the intrusion of assets.

Keywords: network architecture, LTE architecture, smart buses, Internet of Things, ISO / IEC 27033

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día el sistema de transporte público se ha vuelto indispensable en la vida diaria de la mayoría de las personas que necesitan trasladarse desde sus hogares hasta el lugar de trabajo o la escuela.

Los recursos de transporte de superficie convencionales, como vehículos, carreteras, terminales y otra infraestructura de transporte, están quedándose obsoletos. Muchos países se están quedando atrás en la instalación de nueva infraestructura de transporte en sus ciudades. Gracias a los recientes desarrollos en tecnología y la conectividad global habilitada por Internet, los sistemas de transporte están experimentando una profunda transformación que cambiará la forma en que los humanos y los productos se mueven por las ciudades. Es decir, vehículos más inteligentes, más autónomos y más seguros que se comuniquen con otros vehículos y con los edificios de la ciudad, las señales de tráfico y otras infraestructuras serán el estándar de oro [1].

Los ciudadanos que utilizan el sistema público de buses desperdician mucho tiempo esperando el bus en la parada del autobús. En funcionamiento diario de un sistema de bus, el movimiento de autobuses se ve afectado por desconocidas condiciones a medida que avanza el día, como tráfico o despacho de autobuses en irregular tiempo desde la estación. Si la gente que viaja por bus obtuviera la ubicación exacta del bus y la hora aproximada de llegada basada en condiciones normales del tráfico y también el recuento de pasajeros en autobús, con ello aumentara la confiabilidad en el transporte público [2].

Además, se evidencia que los conductores enfrentan muchos problemas para cobrar la tarifa a los pasajeros. Manejar el dinero y devolver el exceso a los pasajeros después de deducir el monto de la tarifa, inspeccionar un pase de viaje se vuelve complejo cuando la congestión, es decir, el número de pasajeros es muy grande, es alta y esta complejidad no se puede administrar de manera efectiva.

El presente proyecto se enfoca en el diseño de una arquitectura de red para que los usuarios de la ciudad de Machala tengan acceso a todos los beneficios del sistema de autobuses inteligentes en el que se transportan, para ello se utiliza la red móvil 4G la cual cuenta con un mayor número de antenas distribuidas por la

ciudad, y también es la red con la mayoría de los dispositivos se conectan, por lo tanto, existe gran cantidad de personas que brindan soporte y mejoras a este tipo de red telefónica.

A todo ello se le debe sumar la inseguridad de las redes, pues al ser un sistema inteligente conectado a internet todo el tiempo, se corre el riesgo de vulnerabilidades en la información, como pérdida de datos, sustracción de cuentas digitales, entre otros sucesos peligrosos para los ciudadanos, por lo que se plantea la implementación de la ISO/IEC 27033 para proteger los datos involucrados en el flujo de información, ésta ISO permite la conservación de la confidencialidad, disponibilidad e integridad de todos los sistemas comprometidos en la aplicación [3].

Además, se especializa en evaluar y aplicar controles que se necesitan para la mitigación de riesgos, así como también la ejecución de buenas prácticas que mejoran la eficiencia, minimizando costos operativos más el ahorro de recursos implementados en los sistemas.

Este proyecto está estructurado en 3 capítulos, en el primero detalla la descripción del contexto del tema y los hechos de interés, además de los requerimientos y el por qué se éste elaborando este tema. El segundo capítulo describe la definición del prototipo, así como también se fundamenta con bases científicas que respalden la información investigada, para lograr alcanzar los objetivos y poner en marcha el proyecto. Finalmente, en el tercer capítulo se establecen los resultados en base al plan de evaluación realizado, y es en donde se concluye y recomienda en base a los objetivos planteados.

CAPÍTULO I. DIAGNÓSTICO DE NECESIDADES Y REQUERIMIENTOS

1.1. Ámbito de aplicación: descripción del contexto y hechos de interés

En las últimas décadas, se ha visto el continuo desarrollo de la tecnología, lo que nos ha llevado a estar en un mundo más conectado y ha cambiado la forma en que se da la interacción entre las personas y cosas. Con el desarrollo de las tecnologías, han surgido nuevos campos de investigación y nuevos servicios innovadores que nos han llevado a la denominada "era digital". [4] En relación con este avance tecnológico, hemos cambiado nuestra forma de vida, y la mayoría de sus aspectos se ven constantemente afectados por este progreso continuo.

Ahora estamos en la era de las cosas inteligentes y la tecnología puede ayudarnos a crear cosas nuevas. Tareas u optimización de acciones y comportamientos que hemos realizado. Un nuevo campo de interés que representa este avance e involucra a los ciudadanos y sus estilos de vida es la llamada "ciudad inteligente". Una ciudad inteligente “se compone de una colección de tecnologías informáticas interconectadas que cooperan para manejar, de una manera más inteligente, diferentes aspectos de los espacios urbanos (por ejemplo, tráfico y movilidad, infraestructuras, seguridad y calidad de vida, etc.)” [4]

El presente trabajo de investigación se enfoca en los sistemas de buses inteligentes. “El transporte público inteligente tiene como objetivo facilitar el transporte de pasajeros y mercancías, de manera que se minimicen los costos en tiempo y dinero y se garantice la seguridad de los pasajeros.”[5] La arquitectura de red que se propone a partir de la investigación realizada, es una red telefónica 4G que permitirá la comunicación entre los medios de transporte urbano (autobuses) de la ciudad de Machala.

Con el fin de mejorar la calidad del servicio del transporte urbano, surge esta propuesta de diseñar una arquitectura de red para el sistema de buses urbano en la ciudad de Machala, ya que el transporte tiene un papel de gran importancia para conectar personas a diferentes lugares.

Para la seguridad, se plantea diseñar la arquitectura de red en base a la ISO/IEC 27033, puesto que es una norma que asegura la integridad y confidencialidad de la información, además de la implementación de controles y buenas prácticas que ayudan a la mitigación de riesgos.

1.2. Establecimiento de requerimientos

Para el diseño de la arquitectura de red se utilizó el software de simulación de redes Cisco Packet Tracer, el cual permite la emulación, configuración y solución de inconvenientes de redes virtuales y también en tiempo real. Antes de empezar la simulación, primero se analiza todas las rutas existentes en la ciudad de Machala, el alcance que tienen en la ciudad y en base a esto poder identificar en qué áreas la conexión a internet se perdería y poder proponer más antenas para estos espacios.

Una vez identificadas éstas áreas, se indaga sobre el tipo de red a implementar, para ello utiliza investigación bibliográfica para conocer el alcance de las mismas, así como también con la ayuda de una aplicación llamada OpenSignal, con ésta aplicación se pudo reafirmar que la red que actualmente tiene mayor alcance en las ciudades es la red 4G por lo que luego de esto se identificó la operadora móvil que tenía más ventajas de conexión, según todo el análisis se pudo evidenciar que la operadora con la que se trabajará será Claro y que ésta tiene un gran número de antenas distribuidas por toda la ciudad por lo que la adquisición de nuevas antenas, sería en menor cantidad.

Luego se diseña la red a implementar con relación a la ISO/IEC 27033 la cual se basa en la seguridad de las redes, en describir todas las amenazas, prácticas y técnicas en el diseño; aspectos en el control de los escenarios que están asociados en una red.

1.3. Justificación del requerimiento a satisfacer

Actualmente y por las circunstancias que se están viviendo a causa de la pandemia, la tecnología se ha tornado imprescindible en la vida diaria de las personas, hoy en día se utiliza el internet para todo, para la educación, trabajo, medicina, socialización familiar, entre otras tareas.

La población se ha vuelto dependiente del uso de internet, cada vez sienten más la necesidad de estar siempre conectados a esta red, incluso cuando viajan, poder estar conectados en todo momento hasta llegar a su destino.

Es por todas estas razones que se pretende realizar una arquitectura de red para que el sistema de buses urbanos de la ciudad de Machala siempre cuente con internet, y con ello poder tener buses inteligentes, que realicen operaciones como: cobro de pasajes, alertas de llegada a su parada, apertura de puertas, información sobre el recorrido de líneas, y no sólo eso, sino también el poder conocer con antelación cuándo llegará su transporte a la parada del autobús, con ello las personas no perderían tiempo en la espera de su medio de movilización, ahorrarían ese tiempo en otras actividades.

En conclusión, todo lo que conlleva la definición de un Smart bus, el poder implementarlo sin la desconfianza de que en ciertos sectores vaya a suceder interferencia o pérdida de datos. Además, se está ayudando a la modernización del transporte, con la optimización de recursos, reducción de costos de transportes, reducción de gastos de combustibles y también mejorando la estabilidad económica del país, al poder contar con un sistema de buses inteligentes, esto generará más turismo en la ciudad, muchas personas preferirán transportarse en un servicio urbano inteligente.

Por último, en la ciudad de Machala no existe un estudio sobre la implementación de una red inalámbrica segura, en la que todos los usuarios se encuentren siempre conectados, por consiguiente, se plantea una base teórica para que próximos investigadores tengan una guía sobre el diseño de una arquitectura de red y que logren poner en marcha sus trabajos a partir de esta investigación.

2. CAPÍTULO II. DESARROLLO DE PROTOTIPO

2.1. Definición del prototipo tecnológico

Para el diseño de la arquitectura de red se realizó un análisis geográfico de la ciudad de Machala, primero para conocer las rutas de buses urbanos que circulan por toda la localidad; identificar los puntos más lejanos a los que llegan, para luego efectuar la disposición de antenas enodoB con el objetivo de que no se pierda la señal en lugares muy remotos.

El desarrollo de esta propuesta empieza con la investigación de Ruta de Buses Urbanos de la ciudad de Machala, esta información se recolectó a través de la página web Movilidad Machala EP http://www.movilidadmachala.gob.ec [6], en donde se puede apreciar que la mayoría de buses accede a la zona céntrica de la urbe, dejando así a los sitios rurales con menos privilegios en cuanto a conectividad, por lo que se propone incrementar el número de antenas que se encuentren ya instaladas. Además, en los sectores rurales la señal se perdería por el hecho de encontrarse en medio de plantaciones de banano, y otros factores que imposibilitan la conexión.

Una vez identificada la trayectoria del autobús, se realizó un análisis en base a estadística para conocer cuál era la operadora de telefonía móvil más idónea para la implementación de este trabajo, según [7], una página multimedia en línea que cubre la industria de las telecomunicaciones, en una investigación realizada hace dos años, indica que la operadora con mayor participación en el mercado del Ecuador es Claro teniendo más accesos prepago u pospago, además, se constató mediante la aplicación OpenSignal [8], la cual proporciona información independiente sobre la conectividad móvil a nivel mundial; que dicha operadora cuenta con un mayor número de antenas ubicadas en el centro de la urbe, por lo que la adquisición de nuevas antenas será en menor volumen.

Finalmente se plantea el diseño de red en base a la norma ISO/IEC 27033 la cual define los lineamientos a seguir para que la red sea segura y mitigar los posibles riesgos que se presenten durante la conexión de los usuarios.

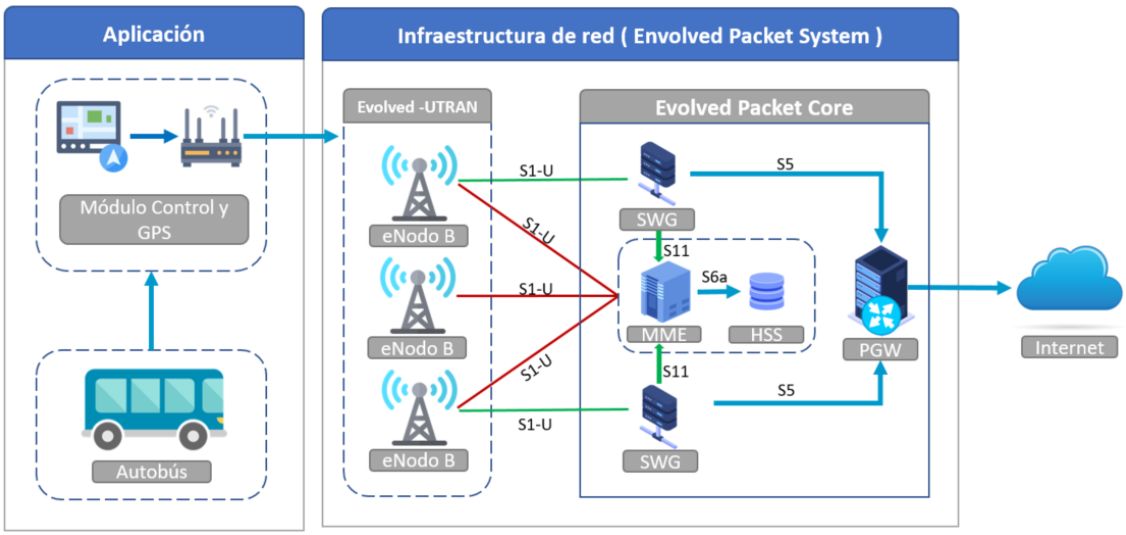


Ilustración 1: Arquitectura del prototipo
Fuente: Elaboración propia

La arquitectura propuesta en la Ilustración 1, indica cómo se realizará la comunicación entre los dispositivos instalados en el bus hacia internet, se trabajara con la operadora móvil claro y utilizando tecnología LTE por lo cual la infraestructura de red que se utilizara será EPS la cual comprende desde el terminal del usuario (UE) la misma que está representada en la capa de aplicación por los módulos de control y GPS instalados dentro de cada unidad, estos a sus vez se interconectara a las estaciones bases que encargara de suministrar la comunicación mediante interfaces de radio las cuales están representadas en la Ilustración 1 con el nombre eNodoB, este a su vez mediante protocolo S1-U se conecta a SGW el mismo que se encargara del ruteo de paquete y referencia al punto de anclaje, este mismo se conecta mediante protocolo S1-MME con lo cual autentica y obtiene la información del usuario almacenada en el HSS, finalmente el SWG se conecta al PWG el cual es el encargado de asignarle una IP al dispositivo y establecer la conexión con internet.

2.2. Fundamentación teórica del prototipo

2.2.1. Internet de las cosas

Una de las primeras definiciones que se da sobre internet de las cosas la da Kevin Ashton quien la define como un sistema capaz de conectar objetos físicos a internet mediante sensores [9].

Los autores [10] definen a internet de las cosas como un conjunto de objetos conectados entre sí que comparten e intercambia datos e información, lo que permite desencadenar una acción en el entorno.

El internet de las cosas también conocido como Iot (Internet of things), dada la existencia se puede encontrar diversos conceptos, pero todos comparten similitudes entre si principalmente se los describe como el conjunto de objetos inteligentes que tienen sensores que interactúan con el medio, y mediante una red comunicación ya se inalámbrica o red cableada envía la información recolectada a un actuador que desencadena una función. En la actualidad y a la gran cantidad de objetos que se le puede dar internet para cumplir una tarea sin la intervención humana ha hecho crecer este concepto a tal magnitud que se lo puede aplicar en cualquier ámbito desde la agricultura, servicios, logística, fabricación, transporte, entre otros [11].

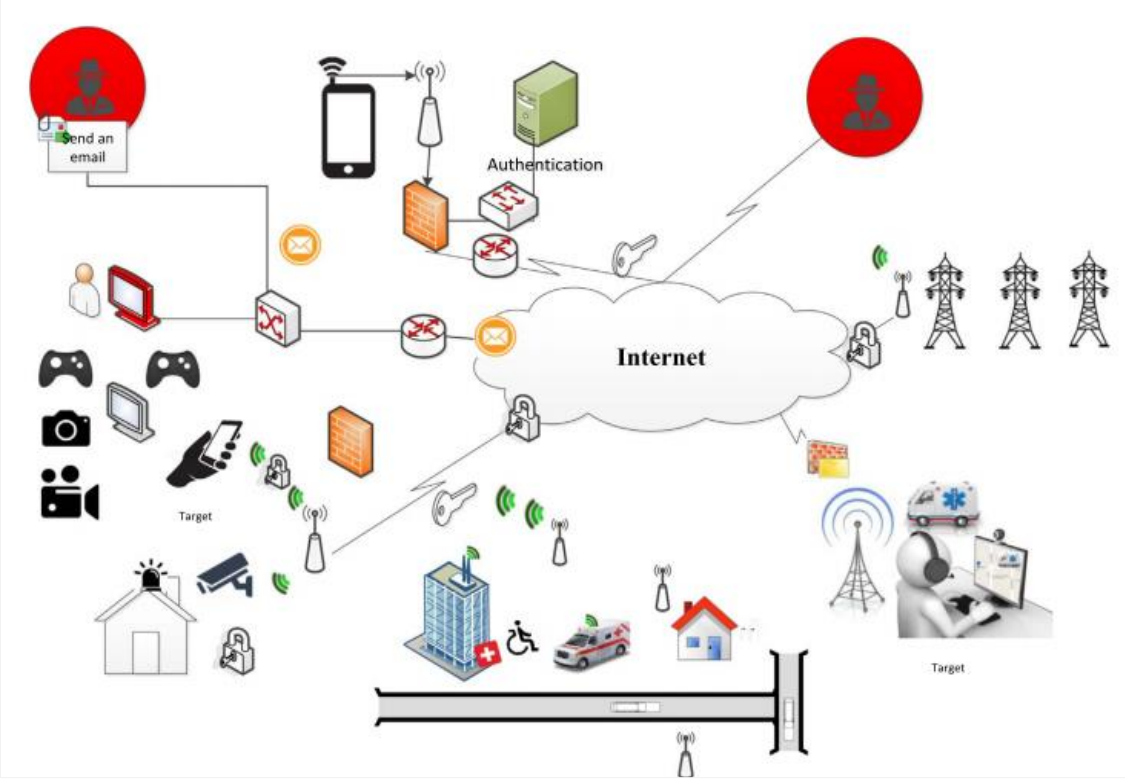


Ilustración 2: Escenario de seguridad de IoT
Fuente: [12]

2.2.2. Smart City

Una Smart City es, una visión compleja y a largo plazo de una mejor zona urbana, con el objetivo de reducir su huella medioambiental y crear una mejor calidad de vida para los ciudadanos. La movilidad es uno de los temas más difíciles de

afrontar en las grandes áreas metropolitanas. Involucra tanto aspectos ambientales como económicos, y necesita tanto alta tecnología como comportamientos de personas virtuosas.

Según [13], la movilidad inteligente está impregnada en gran medida por las TIC, que se utilizan tanto en aplicaciones hacia atrás como hacia adelante, para apoyar la optimización de los flujos de tráfico, pero también para recopilar las opiniones de los ciudadanos sobre la habitabilidad en las ciudades o la calidad de los servicios de transporte público local.

Las principales características de una ciudad inteligente incluyen un alto grado de integración de la tecnología de la información y una aplicación integral de los recursos de información. Los componentes esenciales del desarrollo urbano para una ciudad inteligente deben incluir tecnología inteligente, industria inteligente, servicios inteligentes, gestión inteligente y vida inteligente [14].

Una ciudad inteligente puede monitorear el mundo físico en tiempo real y brindar servicios inteligentes tanto a los residentes locales como a los viajeros en términos de transporte, atención médica, medio ambiente, entretenimiento y energía [15]. Sin embargo, surgen problemas de seguridad y privacidad, ya que las aplicaciones de ciudades inteligentes no solo recopilan una amplia gama de información sensible a la privacidad de las personas y sus círculos sociales, sino que también controlan las instalaciones de la ciudad e influyen en la vida de las personas.

Ilustración 3: Aplicaciones de ciudad inteligente
Fuente: [15]

2.2.3. Smart Transportation

Al hablar de Smart transportation o transporte inteligente, traducido al español, se está involucrando el uso de dispositivos y sensores en el sistema de control del vehículo; por ejemplo, sistema de navegación de automóviles, sistema de gestión de señales de tráfico, sistema de reconocimiento de números y sistema de control de velocidad [16].

El sistema de transporte inteligente consta de varios sensores, que están diseñados para realizar diferentes operaciones sensoriales. Se espera que en la próxima década haya vehículos autónomos que integren una variedad de tecnologías de detección, navegación, control y algoritmos de planificación de movimiento para respaldar el transporte sin conductor.[17]

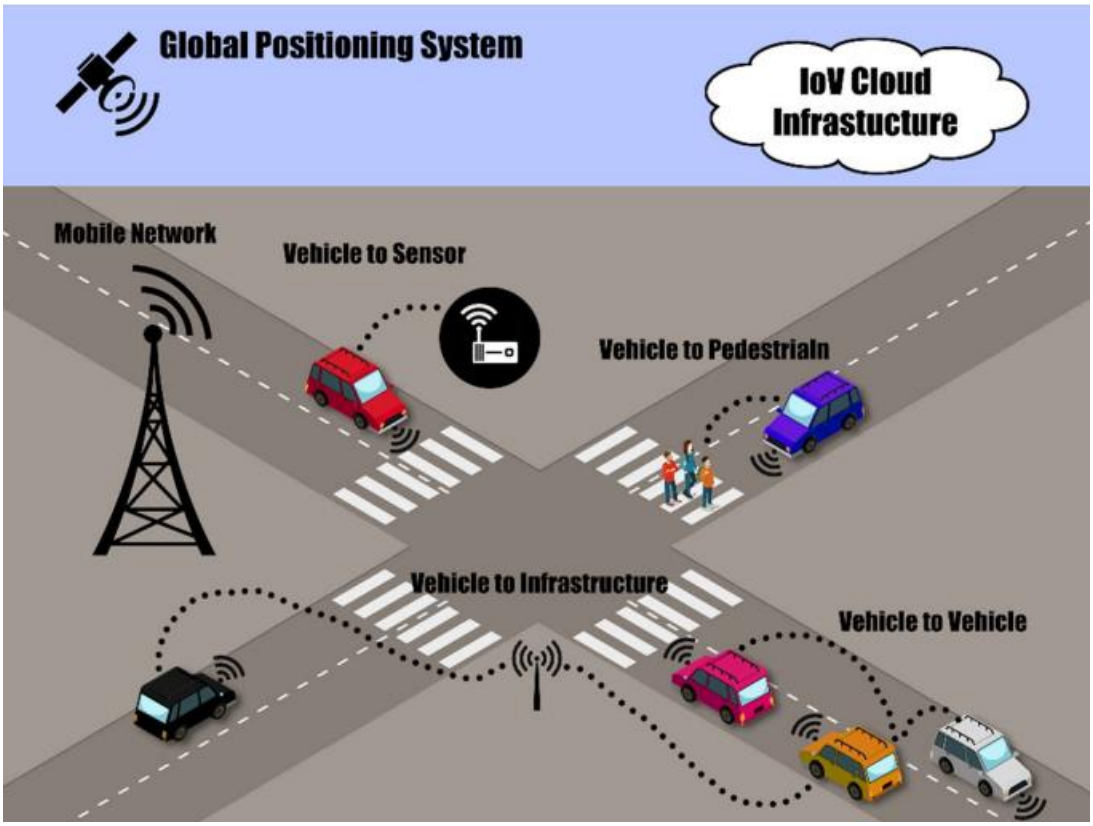


Ilustración 4: Concepto de sistema de transporte inteligente
Fuente:[17]

Para la implementación de un sistema inteligente de transporte se utilizan varios recursos que se detallan a continuación:

2.2.3.1. GPS

[18] considera al GPS como una nueva fuente de recopilación de datos de transporte, especialmente datos de viajes. Los datos de GPS podrían

proporcionar información espacial y temporal en tiempo real. Muestra el comportamiento de viaje, incluida la distancia, la velocidad de viaje, el tiempo de viaje y otra información en formatos digitales al mismo tiempo, lo que podría reducir la carga de informar la información.

2.2.3.2. Fuente de datos de flujo de tráfico

Se instalan sensores y detectores en sitios a lo largo de las carreteras para recopilar datos sobre el volumen de vehículos. Estos datos incluyen características como el flujo de tráfico (volumen / hora), ocupación de carriles y velocidad promedio de los vehículos. Luego, los datos recopilados se analizan utilizando diferentes métodos y modelos para derivar soluciones basadas en datos [18].

2.2.3.3. Tarjeta electrónica

Los datos de la tarjeta inteligente se utilizan para analizar los patrones de viaje personales utilizando herramientas de transporte específicas. La ventaja de utilizar datos de tarjetas inteligentes es que los datos pueden mostrar la hora de inicio, la hora de finalización y la dirección del viaje. Según la frecuencia de los diferentes destinos, el equipo de gestión puede predecir el flujo de tráfico y crear un cronograma adecuado. Sin embargo, dado que los datos de la tarjeta inteligente solo pueden mostrar los datos de tráfico bajo cierto transporte, la flexibilidad de los datos es limitada [18].

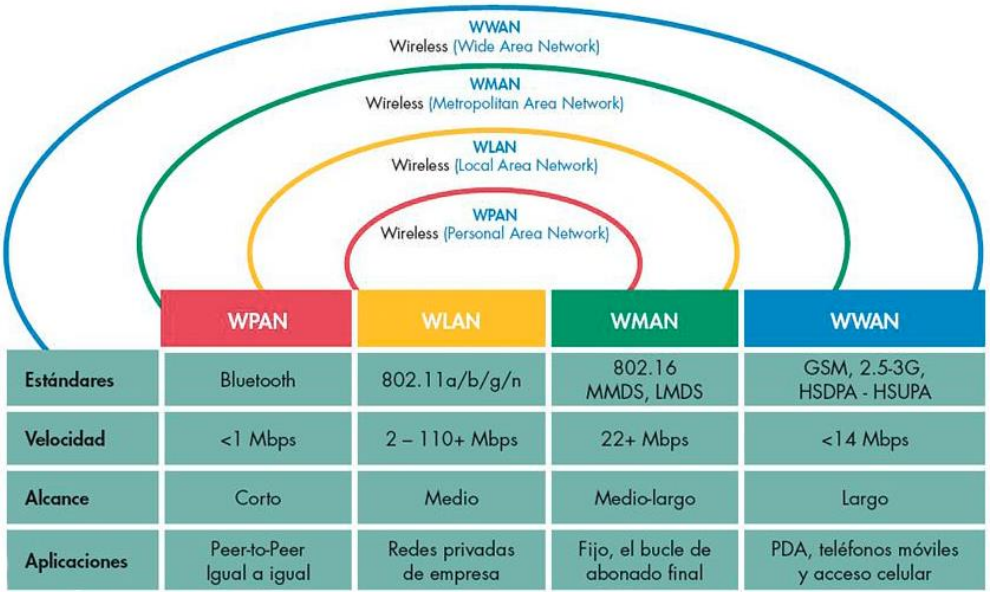
2.2.3.4. Gestión de tráfico inteligente en vehículos conectados

Los vehículos conectados (CV) son muy prometedores para aliviar la congestión del tráfico mediante una gestión inteligente del tráfico. La tecnología CV proporciona datos en tiempo real sobre las condiciones del tráfico que conducen a una mejor gestión del tráfico al mejorar la calidad de los datos.

2.2.4. Redes inalámbricas

Las redes inalámbricas, son un conjunto de dispositivos de tamaños pequeños denominados nodos, nodo-sensor; los cuales están interconectados entre sí. Envían información del espacio inalámbrico hasta un servidor.[19] Estas redes se caracterizan por estar conformadas por nodos, operan con baterías, velocidades bajas de transmisión, además de estar programadas por largos periodos de tiempo. También se destaca que es una tecnología empleada en el

Internet de las Cosas (IoT).[20] Una red inalámbrica permite que los dispositivos permanezcan conectados a la red pero que se muevan sin ataduras a ningún cable.



	WPAN	WLAN	WMAN	WWAN
Estándares	Bluetooth	802.11a/b/g/n	802.16 MMDS, LMDS	GSM, 2.5-3G, HSDPA - HSUPA
Velocidad	<1 Mbps	2 – 110+ Mbps	22+ Mbps	<14 Mbps
Alcance	Corto	Medio	Medio-largo	Largo
Aplicaciones	Peer-to-Peer Igual a igual	Redes privadas de empresa	Fijo, el bucle de abonado final	PDA, teléfonos móviles y acceso celular

Ilustración 5: Tipos redes inalámbricas
Fuente:[21]

2.2.4.1 Tipos de conexiones inalámbricas

2.2.4.1.1 Wireless Personal-Area Networks (WPAN)

Este tipo de red normalmente abarcaría solo unos pocos metros alrededor de un individuo. Las comunicaciones por infrarrojos (IRDA) y el cada vez más popular Bluetooth son tecnologías de implementación de WPAN comunes. ZigBee está emergiendo como otra opción WPAN.[22]

2.2.4.1.1 Wireless Local-Area Network (WLAN)

En este caso, el alcance de la red es algo así como un edificio. Podría ser solo parte de un edificio o podría abarcar un pequeño grupo de edificios. Se puede cubrir una tienda o restaurante utilizando una WLAN. Normalmente, una zona de este tipo se denomina "punto de acceso inalámbrico. La tecnología WLAN se utiliza para ahorrar costos y evitar el tendido de cables, mientras que en otros casos es la única opción para brindar acceso a Internet de alta velocidad al público.[23]

2.2.4.1.1 Wireless Metropolitan-Area Network (WMAN)

WMAN permite la conexión de varias redes dentro de un área metropolitana (como diferentes edificios dentro de la misma ciudad) y proporciona una alternativa o respaldo al cableado estructurado. [23]

2.2.4.1.1 Wireless Wide-Area Network (WWAN)

Este tipo de red proporciona acceso a Internet y a la red en grandes áreas (es decir, ciudades o países) mediante sistemas satelitales o sitios de antenas mantenidos por un ISP. También se conocen comosistemas2G o 2ª Generación. Las tres principales tecnologías WAN inalámbricas comprenden los dos sistemas celulares tradicionales, GSM y CDMA, y el WiMAX más nuevo. GSM y CDMA utilizan HSPA y EV-DO para ofrecer velocidades de datos 3G. WiMAX ofrece un servicio de datos más rápido.[23]

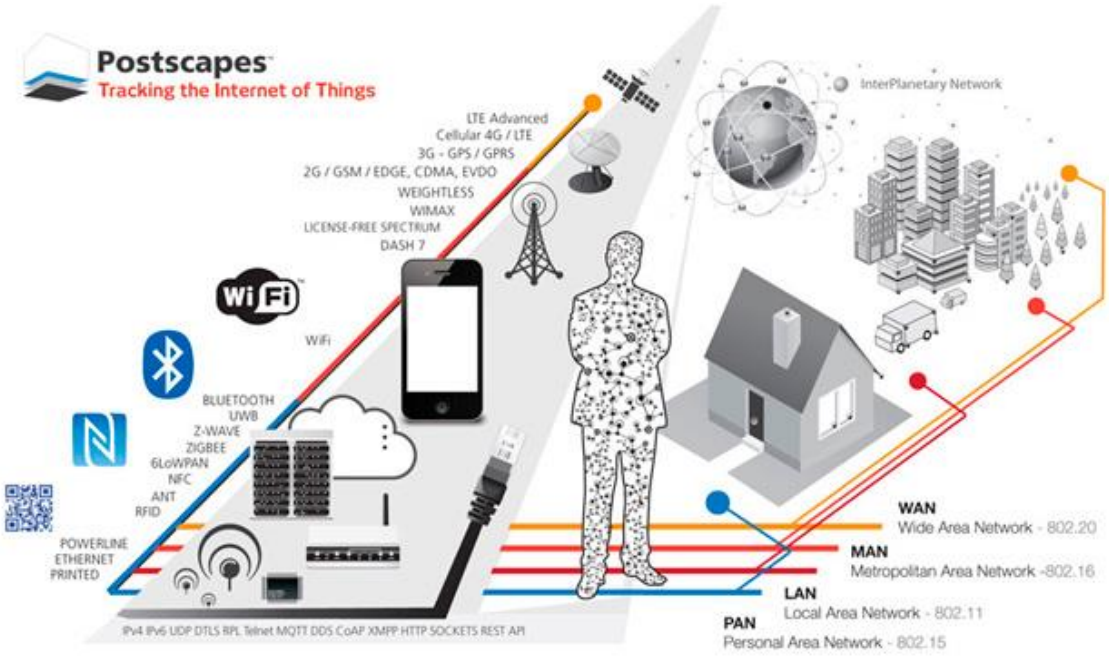


Ilustración 6: Tipos de redes inalámbricas
Fuente:[24]

2.2.5. Arquitectura de red

La arquitectura de red es el diseño de la red. Una red consta de equipos de transmisión, protocolos de comunicación, software e infraestructura. Los arquitectos de red se aseguran de que la conectividad entre los componentes sea ininterrumpida. El diagrama de la arquitectura de la red proporciona una imagen completa de la red establecida con una vista detallada de todos los recursos accesibles.[25]

2.2.5.1. Arquitectura ITS

La creación de una arquitectura telemática de transporte es lograr la interoperabilidad entre aplicaciones telemáticas individuales, incluido el uso máximo de la infraestructura disponible por todas las aplicaciones telemáticas, manteniendo su propio requisito del sistema (requisitos técnicos: seguridad,

fiabilidad, disponibilidad, integridad, etc.) y requisitos relacionados con el transporte. Además, se considera cuatro criterios para su creación asequibilidad, compatibilidad e integración regional, geopolítica y aspectos técnicos.[26]

2.2.6. Redes móviles

Las redes celulares son altamente eficientes en el uso del espectro electromagnético, pueden cubrir una gran área geográfica de ondas de radio, pueden reutilizar canales de radio y redistribuirlos a varias áreas de cobertura (llamadas células co-canal). La interferencia entre celdas se ve atenuada por el espaciamiento co-canal en la celda. Cada celda está controlada por un transductor, que se llama estación base, abreviado como BS. En la ilustración 1 puede ver un ejemplo de topología de red celular. [27]

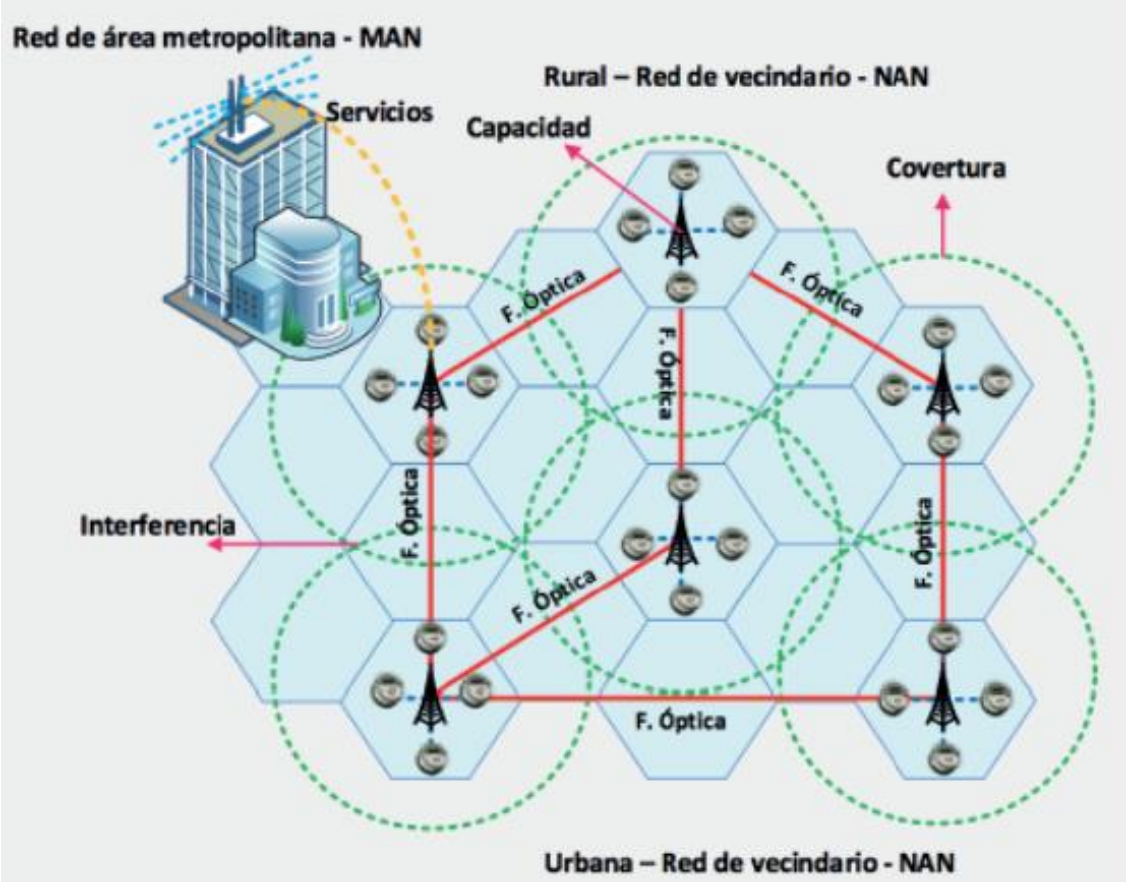


Ilustración 7: Infraestructura Red Móvil
Fuente:[27]

2.2.6.1 Arquitectura general de una red móvil

2.2.6.1.1 Celdas o células

Una celda es la unidad geográfica de una red móvil. El término "celda" proviene de la estructura hexagonal formada por las abejas en sus panales. Son las áreas

geográficas donde la estación base transmite y recibe, y generalmente están representadas por hexágonos. Debido a las restricciones impuestas por el terreno y la topografía de las construcciones hechas por el hombre, la planta real de una unidad no suele coincidir con el círculo y mucho menos con el hexágono.[28]

2.2.6.1.2 Clusters o racimo

Un clusters es un grupo de celdas consecutivas. Esta es la estructura básica que se repite en toda el área de cobertura. Su tamaño y diseño tienen mucho que ver con el concepto de reutilización de frecuencias, lo veremos a continuación, que es la base para entender la arquitectura del sistema celular. [28]

2.2.6.1.3 Reutilización de frecuencias

El concepto de teléfono celular está estrechamente relacionado con la planificación del operador o la reutilización de frecuencias. La reutilización de frecuencias se basa en la asignación de un conjunto de portadoras que se utilizarán en el área de cobertura de esa celda para cada celda. Para evitar interferencias que compliquen la comunicación, las celdas vecinas nunca usarán la misma frecuencia.[28]

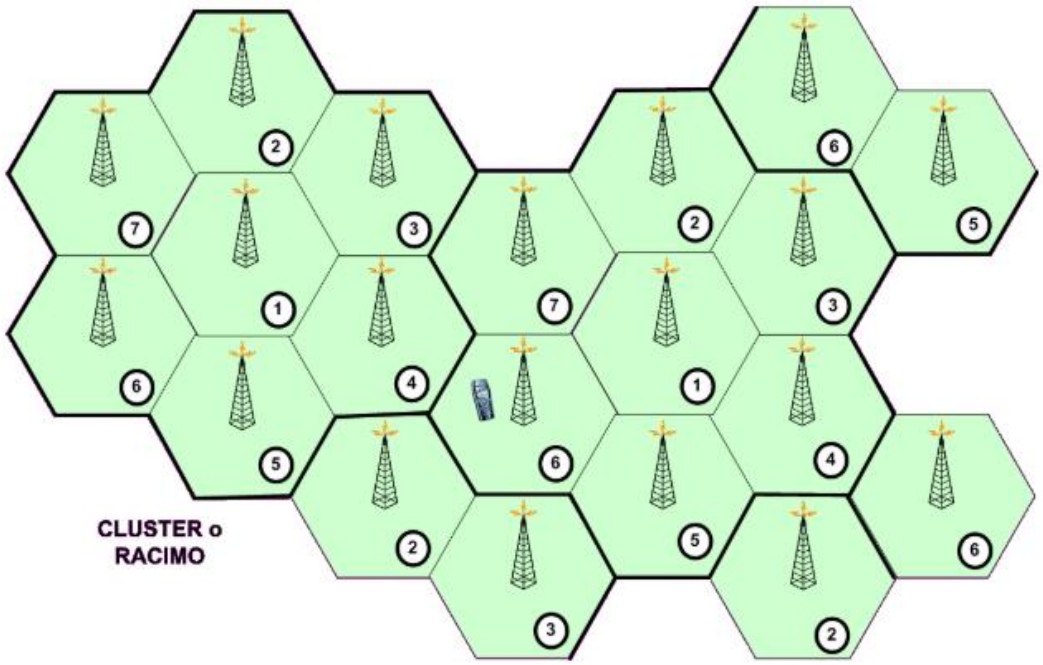


Ilustración 8: Frecuencia redes móviles
Fuente:[28]

2.2.6.1.4 División de celdas

A consecuencia de aspectos económicas y de diseño, no se puede realizar el concepto de crear un sistema compuesto enteramente por muchas celdas pequeñas de tamaño similar. Para superar esta dificultad, los operadores introdujeron el concepto de división celular. Esta estrategia implica dividir las células con mayor concentración de usuarios en células más pequeñas. Su uso es particularmente evidente en áreas urbanas donde la concentración de residentes urbanos es muy diferente y cambia mucho a medio plazo. [28]

Suelen diferenciarse tres tamaños de células: “Macroceldas: para zonas de cobertura grandes con usuarios de gran movilidad. Microceldas: para zonas urbanas reducidas (200-400 m) y usuarios de movilidad baja. Picoceldas: para cobertura de zonas interiores (70-80 m) y usuarios de movilidad reducida.” [28]

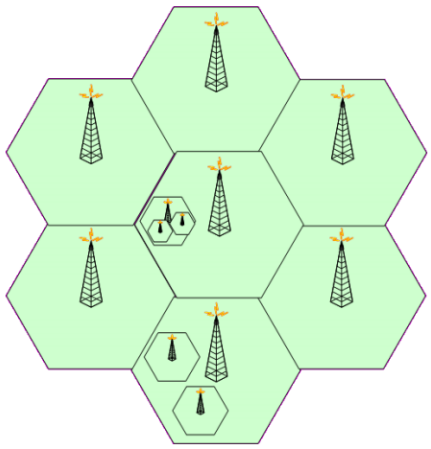


Ilustración 9: División de celdas
Fuente: [28]

2.2.6.1.5 Traspasos (Handovers)

El último obstáculo en el despliegue de redes móviles proviene de la posibilidad de que los usuarios se muevan entre celdas. Si esto sucede y no está utilizando un terminal para comunicarse, la red solo necesita mantener un registro en caso de que pueda encontrar su ubicación cuando llegue una llamada o mensaje.[28]

2.2.6.2. Tipos de Redes móviles

2.2.6.1.1. GSM

GSM juega un papel clave en el proceso de recepción y transmisión de información en seguridad inalámbrica controle las redes que afectarán la

distancia de comunicación, el consumo de energía del nodo, la estabilidad de la red y otros indicadores directamente.

El costo de instalación y mantenimiento de un sistema de seguridad para el hogar basado en GSM es mucho más económico que otros sistemas de seguridad para el hogar, también es muy flexible y duradero [29].

2.2.6.1.1.1 Arquitectura de una red GSM

La red GSM surge con el desarrollo de la arquitectura celular, en esta red se destaca tres aspectos esenciales:

- Estación móvil (Mobile Station, MS)
- Subsistemas de estación base (Base Station Subsystem, BSS)
- Subsistemas de red (Network Subsystem, NSS)

La estación móvil consta de equipos de usuario o teléfonos móviles con tarjetas SIM. Los cinco componentes principales del subsistema de conmutación de red (NSS) son: AuC, HLR, VLR, MSC y EIR. El subsistema de la estación base (BSS) tiene dos componentes principales, a saber, el controlador de la estación base (BSC) y muchas estaciones transceptoras base (BTS). En la figura x se puede observar un ejemplo de arquitectura de red GSM.[30]

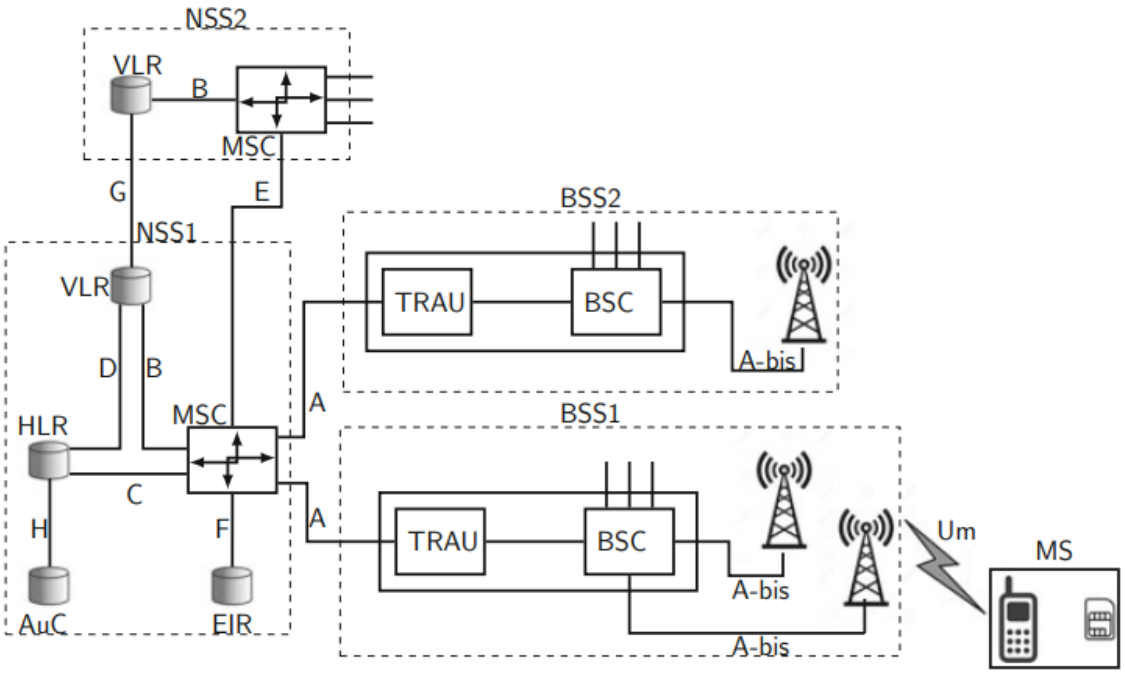


Ilustración 10: Arquitectura de una red GSM
Fuente:[30]

Estación móvil (Mobile Station, MS)

“Es el nombre estandarizado que recibe el dispositivo móvil para la comunicación vía RF (Radio Frequency).”[31]

Teléfono móvil (MH), “El dispositivo o MH es esencialmente una unidad combinada que se utiliza para la transmisión y recepción de datos de voz, y su circuito es responsable de:”[30]

- Sincronizaciones de tiempo y frecuencia,
- Medir y reportar las intensidades de la señal de BTS,
- Codificación de voz y mensajes,
- Códigos de corrección de errores para transmisión por aire, y
- Comprimir y descomprimir datos y voz

Base Station Subsystem

BSS se compone de tres partes: transceptor de estación base (BTS) o estación base (BS), Controlador de estación base (BSC) y transcodificador y unidad de adaptación de frecuencia (TRAU).

BTS Proporciona conexión de última milla con MS. Además, el equipo de comunicación debido a que es responsable de comunicarse con la MS, es la clave en el área de servicio celular. Realiza las funciones de antena, módem y procesamiento de señales. El BSC gestiona los recursos de radio de una o más BS. Administrar la configuración del canal y también sirve como interfaz entre Mobile Switching Center (MSC) y su BS. Sin embargo, una de las tareas importantes de BSC es actuar como centro. TRAU producirá un ruido agradable, que coincida con el ruido de fondo, al final del receptor indica que el transmisor no ha fallado. [30]

Base Transceiver Station (BTS)

Son las estaciones base o celdas que brindan la conectividad con un MS mediante la interfaz de aire Um del estándar GSM.”[31]

Base Station Controller (BSC)

“En este nodo se encuentra el equipamiento que controla un grupo de estaciones base (BTS), además de otras funciones como el control de potencia emitido por los usuarios.”[31]

Network and Switching Subsystem (NSS)

NSS es responsable de las funciones de conmutación, el posicionamiento MS y la interconexión con otras redes. Consiste en un centro de conmutación móvil (MSC), un registro de ubicación de origen (HLR), un registro de ubicación de visitantes (VLR) y un centro de conmutación móvil de puerta de enlace (GMSC).

El MSC es el elemento principal del NSS, controla los diferentes BSC y es responsable del enrutamiento de las llamadas entrantes / salientes y de las funciones de movilidad del terminal, como el registro y la ubicación de la MS. HLR es una base de datos estática, que contiene parámetros específicos del usuario (información de ubicación, servicios autorizados, tipos de terminales, etc.); VLR es una base de datos dinámica, asociada al MSC, que almacena información sobre los terminales registrados en el MSC. Cuando la MS está registrada en la red, el VLR correspondiente usa el HLR de la red local para verificar diferentes parámetros. GMSC es el punto de interconexión entre la red GSM y la red externa que le proporciona la función de puerta de enlace.[32]

Mobile Services Switching Center MSC

“Es el primer nodo del núcleo de toda la red, se encarga de la asignación de los canales de tráfico (TCH) a los abonados, sincronizando el time slot adecuado para cada comunicación. Además, realiza los procedimientos de enrutamiento.” [31]

Home Location Register HLR

“Es una base de datos, al igual que EIR, también está conectada a MSC. Su función se basa en alojar información sobre la ubicación de los dispositivos en la red y los servicios a los que pueden acceder, es decir, contiene datos sobre la capacidad de consumo de los dispositivos de todos los usuarios de la red.” [31]

Visited Location Register (VLR)

La base de datos LAC (location area call) encargada de registrar un grupo de usuarios es la ubicación que brinda cobertura al terminal. Además, también puede obtener una copia de la información HLR cuando el dispositivo está activo, así como otras funciones auxiliares. El VLR es responsable de un grupo de áreas específicas y almacena los datos de todos los usuarios que se encuentran actualmente en estas áreas. Generalmente, cada red tiene un HLR central y cada MSC tiene un VLR. [31]

Authentication Center AuC

El centro de verificación de identidad es una base de datos que se utiliza como centro de verificación de identidad. El MSC y el HLR lo consultan constantemente para conocer la autoridad del usuario para acceder a la red. Este proceso lo realiza el SIM (Subscriber Identity Module), que es propiedad de cada móvil dispositivo.[31]

Equipment Identy Register EIR

Al mismo tiempo, el EIR almacena el número de serie proporcionado por el fabricante del terminal (IMEI) para que pueda verificar o bloquear el acceso al servicio a las estaciones móviles notificadas como robadas. EIR es una base de datos interconectada con el MSC, que almacena toda la información relacionada con el estado del dispositivo móvil de cada suscriptor.[31]

2.2.6.1.2. 3G

UMTS Universal Mobile Telecommunications System, para satisfacer la demanda cada vez mayor de transmisión de datos, se han optimizado las tecnologías de próxima generación para lograr la transmisión de datos en la capa inalámbrica. Además, UMTS ha agregado nuevas características de seguridad, como autenticación mutua y nuevos algoritmos de encriptación. Aunque la red está conmutada por paquetes en su núcleo, la transmisión de voz y SMS todavía se proporciona como servicios de red separados.[33]

2.2.6.1.3. 4G LTE

LTE “proporciona una tecnología que puede soportar alta velocidad de transmisión, mayor eficiencia de espectro, retardo reducido, eficiencia de uso del

espectro y otras tecnologías de acceso de radio 3GPP (GSM, WCDMA / HSPA).”[34]

Es un tipo de red móvil utilizado por las telefonías móviles de cuarta generación Long Term Evolution (LTE) para lograr una tasa de transferencia óptima en cuanto a envío de datos mediante el uso de múltiples sub-portadoras ortogonales entre sí (Orthogonal Frequency Divison Multiplex, OFDM y su variante de acceso al medio, OFDMA), las cuales son moduladas por flujos de datos a tasas relativamente bajas. Adicionalmente, considera el uso de múltiples transmisores y receptores (Multiple Input Multiple Output, MIMO). De este modo, se logran tasas de datos teóricas de 100 Mbps en downlink con ancho espectral de 20 MHz [35].

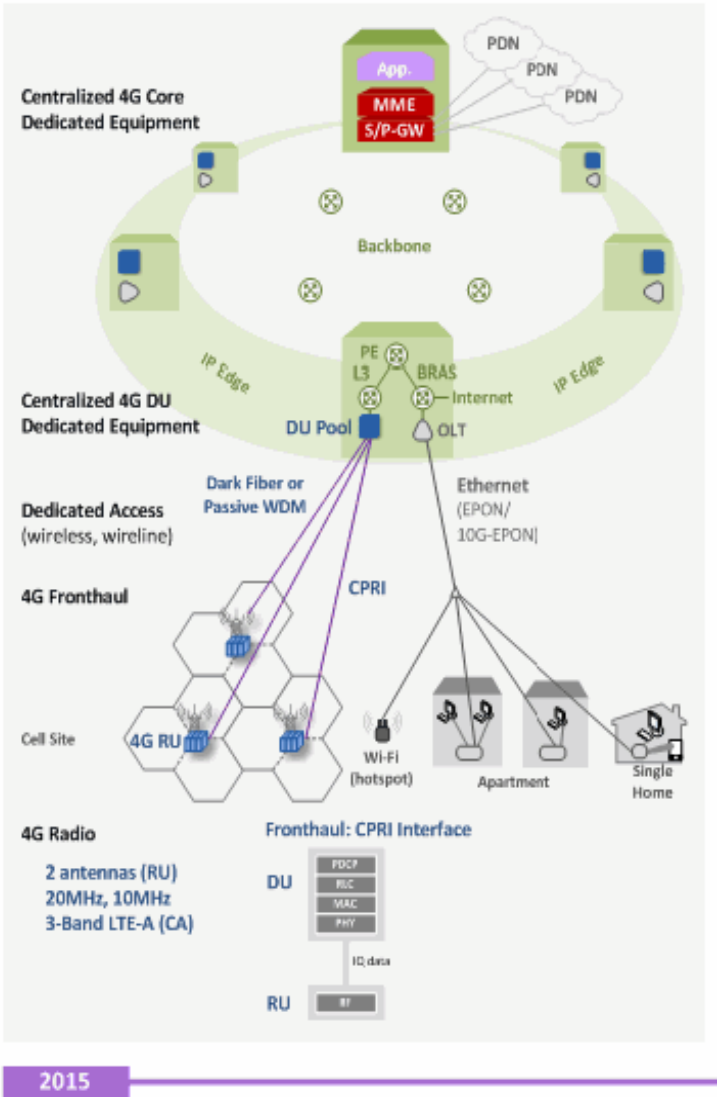


Ilustración 11: Red móvil 4G
Fuente: [36]

2.2.6.1.3.1 Arquitectura de una red LTE

- Enhanced Node B - eNode B (eNB)

  La red eNB es la estación base responsable de la gestión del protocolo de interfaz aérea (Uu). Además, también combinan las funciones de la estación base y el controlador (controlador de red radio) diseñado en la tercera generación (3G), Nodo B y RNC. Las funciones principales son asignación de recursos, control de potencia, traspaso, señalización, etc. [31]

- Home Subscriber Server (HSS):
  HSS “es la única base de datos en la nueva arquitectura de red, que agrega todas las funciones de la base de datos (HLR, VLR, EiR, AuC), como identificación del usuario, estado del dispositivo móvil, información del usuario, etc.” [31]
- Mobility Management Entity (MME)
  MME “es un nodo evolucionado del SGSN de segunda generación, aunque se agrega una función de lista para monitorear la administración de suscriptores y la selección de pasarelas en conexión con otras redes.”[31]
- Serving Gateway (SGW)
  SGW es un nodo muy importante porque es responsable de enrutar todos los paquetes de datos entre Eutran y EPC. Tienen una conexión directa con el nodo ENodeB a través de la interfaz S1-U, una de sus funciones es el anclaje del traspaso, y lo mismo ocurre cuando este proceso ocurre en otras infraestructuras además del ENodeB. [31]
- Packet Data Network Gateway (PGW)

  PGW “es un nodo que protege la información interna de la red del operador, pues si bien su función principal es la de interconectarse con la red externa PDN (Packet Data Network), también cuenta con sistemas como un firewall de alta seguridad para proteger la red.” [31]

2.2.6.1.4. 5G

5G es la tecnología de comunicación móvil de próxima generación diseñada para proporcionar una mayor capacidad y velocidades de datos más altas que la generación anterior Long Term Evolution (LTE). La tecnología 5G, promete una

latencia ultrabaja y una fiabilidad ultra alta, lo que permite servicios innovadores en diferentes sectores industriales [37].

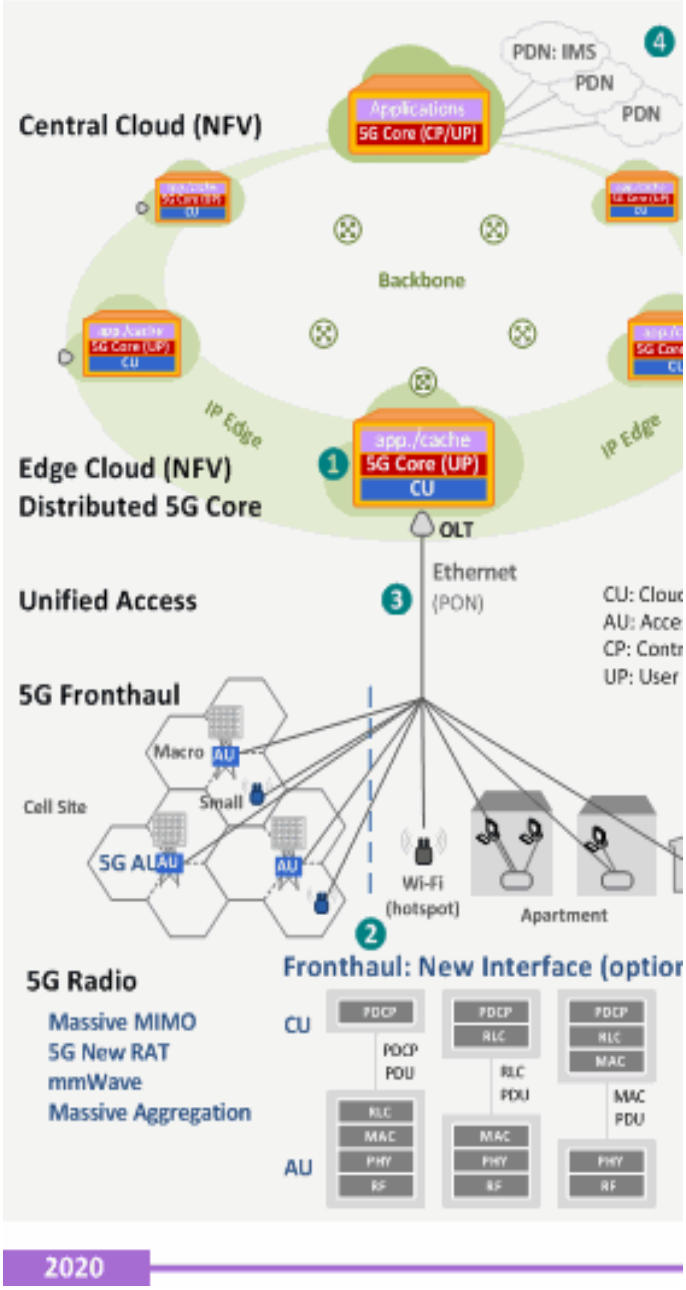


Ilustración 12: Red móvil 5G
Fuente: [36]

2.2.7. Tecnología Inalámbrica Wimax

Es una conexión WMAN inalámbrica de alta velocidad y de larga distancia. Autoriza un caudal de 70 Mb / s en un máximo de 50 km. El WiMax puede operar en modo punto a multipunto, es decir el modo de infraestructura que se conoce por Wi-Fi [38].

El entorno WiMAX “tiene amplia diversidad de programación de QoS debido a su variabilidad con respecto al uso de información en tiempo real, como es el caso del UGS (Unsolicited Grant Service), la configuración de sus flujos para enviar paquetes de tamaño fijo en intervalos recurrentes con la menor latencia y fluctuación posible desde flujos en clases de schedulling, en donde los flujos de paquetes de información UGS son priorizados sobre los flujos de rtPS, nrtPS, BE y ErtPS.”[39]

Ilustración 13: Tecnología Wimax
Fuente:[40]

2.2.8. Simulador de red Cisco Packet Tracer

Cisco Packet Tracer es una herramienta enfocada en la enseñanza y de simulaciones de red. Además, se puede utilizar con fines de generar reformas IoT. Entre las funciones más destacadas podemos mencionar las siguientes.[41]

- Enseñanza de simulaciones de red entre los estudiantes
- Permite que se explore la temática de Internet de las cosas.
- Construir redes desde simples hasta complejas, etc.

2.2.9. ISO/IEC 27001

“Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.” [42]

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información de la empresa. Para hacer esto, investiga los problemas potenciales que pueden afectar la información (es decir, la evaluación de riesgos) y luego definir qué medidas deben tomarse para evitar que ocurran estos problemas.

Ilustración 14: Estructura ISO 27001
Fuente: [37]

2.2.10. ISO/IEC 27033

I ISO/IEC 27033 es un estándar de varias partes derivado del existente ISO/EC 18028 de cinco partes. Se enfoca en describir todas las amenazas, prácticas y técnicas en el diseño; aspectos en el control de los escenarios que están asociados en una red. Para cada escenario se provee orientación detallada sobre las amenazas de seguridad, las técnicas y controles de diseño de seguridad requeridos para mitigar los riesgos asocia.[43]

2.2.10.1 ISO/IEC 27033-1 Conceptos y descripción general de la seguridad de la red.

Proporciona una hoja de ruta y una descripción general de los conceptos y principios que sustentan las partes restantes de ISO / IEC 27033. Definir y describir los conceptos asociados con la seguridad de la red y proporcionar una guía de gestión sobre la misma. Esto incluye la provisión de una descripción general de la seguridad de la red y las definiciones relacionadas, y orientación sobre cómo identificar y analizar los riesgos de seguridad de la red y luego definir los requisitos de seguridad de la red. También presenta cómo lograr arquitecturas de seguridad técnica de buena calidad, y los aspectos de riesgo, diseño y control asociados con la red típica escenarios y áreas de “tecnología” de red. [44]

2.2.10.2 ISO/IEC 27033-2. Directrices para el diseño e implementación de seguridad de red.

Definir cómo las organizaciones deben lograr arquitecturas, diseños e implementaciones de seguridad técnica de red de calidad que garanticen la seguridad de la red adecuada a sus entornos comerciales, utilizando un enfoque coherente para la planificación, el diseño y la implementación de la seguridad de la red, según corresponda, con la ayuda del uso de odels./frameworks y es relevante para todo el personal que participa en la planificación, el diseño e implementación de los aspectos arquitectónicos de la seguridad de la red (por ejemplo, arquitectos y diseñadores de redes, administradores de redes y oficiales de seguridad de redes).[44]

2.2.10.3 ISO/IEC 27033-3. Escenarios de redes de referencia: amenazas, técnicas de diseño y problemas de control.

El definir los riesgos específicos, técnicas de diseño y problemas que se pueden presentar en el control sobre los escenarios de red, es su principal enfoque. Es relevante para todo el personal involucrado en la planificación, diseño e implementación de los aspectos arquitectónicos de la seguridad de la red.[44]

2.2.10.4 ISO/IEC 27033-4. Protección de las comunicaciones entre redes mediante pasarelas de seguridad

Proporciona una descripción general de las puertas de enlace de seguridad a través de una descripción de diferentes arquitecturas. Describe cómo las puertas

de enlace de seguridad analizan y controlan el tráfico de la red mediante: Filtrado de paquetes; Inspección de paquetes con estado; Proxy de aplicaciones (firewalls de aplicaciones); Traducción de direcciones de red NAT; Análisis y filtrado de contenido.[44]

2.2.10.5 ISO/IEC 27033-5 Protección de las comunicaciones a través de redes mediante redes privadas virtuales (VPN)

Pautas para la selección, implementación y monitoreo de los controles técnicos necesarios para brindar seguridad de red utilizando conexiones de Red Privada Virtual (VPN) para interconectar redes y conectar usuarios remotos a redes. roporciona orientación para asegurar el acceso remoto a través de redes públicas. Ofrece una evaluación incompleta de alto nivel de las amenazas a las VPN. Introduce diferentes tipos de acceso remoto, incluidos protocolos, problemas de autenticación y soporte al configurar el acceso remoto de forma segura.[44]

2.2.10.6 ISO/IEC 27033-6 Asegurar el acceso a la red IP inalámbrica

Define los riesgos específicos, diseñar técnicas y aspectos de control para asegurar las redes inalámbricas IP. Ofrece consejos básicos para WiFi, Bluetooth, 3G y otras redes inalámbricas. Aquí se enumeran varias amenazas que por lo general son modos de ataque o riegos en los escenarios de red. El estándar indica que el cifrado es un control de integridad.[44]

Modelo PHVA

[45] define al modelo PHVA como una herramienta de gestión introducida por el estadístico estadounidense Edward Deming en la década de 1950. El acrónimo del ciclo o fórmula PHVA forma un acrónimo que consiste en las abreviaturas de las palabras Plan, Hacer, Verificar y Actuar. Cada una de estas cuatro definiciones corresponde a una fase o fase del ciclo:

Planificación: En la fase de planificación, las metas se plantean de acuerdo con la estrategia de la organización y se determinan los procesos necesarios para lograr ciertos resultados. En esta etapa, también se determinarán los parámetros de medición utilizados para controlar y monitorear el proceso [45].

Hacer: Incluye la implementación de los cambios o acciones necesarias para lograr la mejora propuesta. Con el fin de mejorar la eficiencia y poder corregir fácilmente los errores que puedan ocurrir en el proceso de ejecución, un plan de prueba generalmente se formula como un testeo o un plan piloto a modo de prueba [45].

Verificación: Luego de implementar el plan de mejora, se establecerá un período de prueba para medir y evaluar la efectividad de los cambios. Esta es una etapa de ajuste y ajuste [45].

Acción: Una vez realizada la medición, si el resultado no cumple con las metas esperadas y predeterminadas, realice las correcciones y modificaciones necesarias. Por otro lado, se tomaron decisiones y acciones relevantes para mejorar continuamente el desarrollo del proceso [45].

2.3. Objetivos del Prototipo

2.3.1. Objetivo General

Diseñar una arquitectura de red mediante la ISO/IEC 27033 para un sistema de buses inteligentes en la ciudad de Machala.

2.3.2. Objetivos Específicos

- Realizar una investigación bibliográfica analizando la información digital que servirá de base teórica para la realización del proyecto.
- Identificar tecnologías inalámbricas que permitan el envío de datos en dispositivos en movimiento.
- Determinar la infraestructura de red más adecuada que se adapte a la tecnología existente en nuestra ciudad.

2.4. Diseño del Prototipo

Para la elaboración de la arquitectura de red se realizó un análisis geográfico de la ciudad de Machala, además de la simulación de la red por la cual los buses se conectarían.

2.4.1. Análisis Geográfico

En este punto se ha efectuado el estudio de la localización en donde se va a implementar la arquitectura de red para que los buses urbanos tengan conexión a internet, todo ello mediante tecnología 4G, el estudio comprende todas parroquias del cantón Machala: Machala, Puerto Bolívar, La Providencia, 9 de mayo, Jubones, Jambelí, El Cambio y El Retiro (rural), enfocándose en los sectores en donde circulen los buses urbanos de la ciudad.

Para este análisis se accedió a la página de movilidad en donde se obtuvieron todas las rutas actualmente disponibles. Luego se procedió a unir todas las rutas de los buses en un solo mapa, ya que en la página web estas rutas se encuentran, en un mapa diferente para cada ruta de recorrido de bus. (Ver Anexo A).

La ciudad cada día crece más en cuanto a construcciones, por lo que las líneas de buses han ido incrementando su recorrido, por poner un ejemplo la línea 14 ahora llega hasta el sitio Ceibales, lo que hasta hace algunos años eso sería un sueño, también la línea 18 que en la actualidad llega hasta el sitio La Iberia, y no decir de la línea 20 que ingresa hasta la parroquia más alejada del cantón, se hace énfasis en estas líneas porque éstas circulan por sectores en donde aún no se encuentran totalmente habitados, y por ende las operadoras telefónicas no invierten en la implementación de antenas enodoB.

2.4.2. Análisis de redes de Operadoras Telefónicas.

En ecuador existe tres operadoras móviles que predominan el mercado tal y como se describe en la tabla N°1, en el cual se logra observa los distintos espectros en los que trabaja cada operadora, adicionalmente del porcentaje que domina en el mercado ecuatoriano.

Operadora Telefónica	Servicios	Tecnología y frecuencia	Porcentaje de mercado
Claro	Red telefónica e interne móvil	850MHz–1900MHz GSM; 850MHz–1900MHz UMTE/HSPA;	53,6 %

		1700/2100 MHz LTE	
CNT	Red telefónica e interne móvil	1900 MHz GSM; 1900 MHz UMTS / HSPA; LTE 1700/2100MHz 700MHz	28,1 %
Movistar	Red telefónica e interne móvil	850MHz–1900MHz GSM; 850MHz–1900MHz UMTE/HSPA; 1900MHz LTE	18,3%

Tabla 1: Operadores móviles en el Ecuador
Fuente: [7]

En la siguiente ilustración se logra observar que la operadora móvil que tiene más impacto en el Ecuador es Claro dominándolo con el 53,6% del mercado total, por lo que se deduce que es la operadora con mayor número de usuarios en el país. Mientras que las operadoras Movistar y CNT tiene un menor porcentaje de acogida de usuarios.

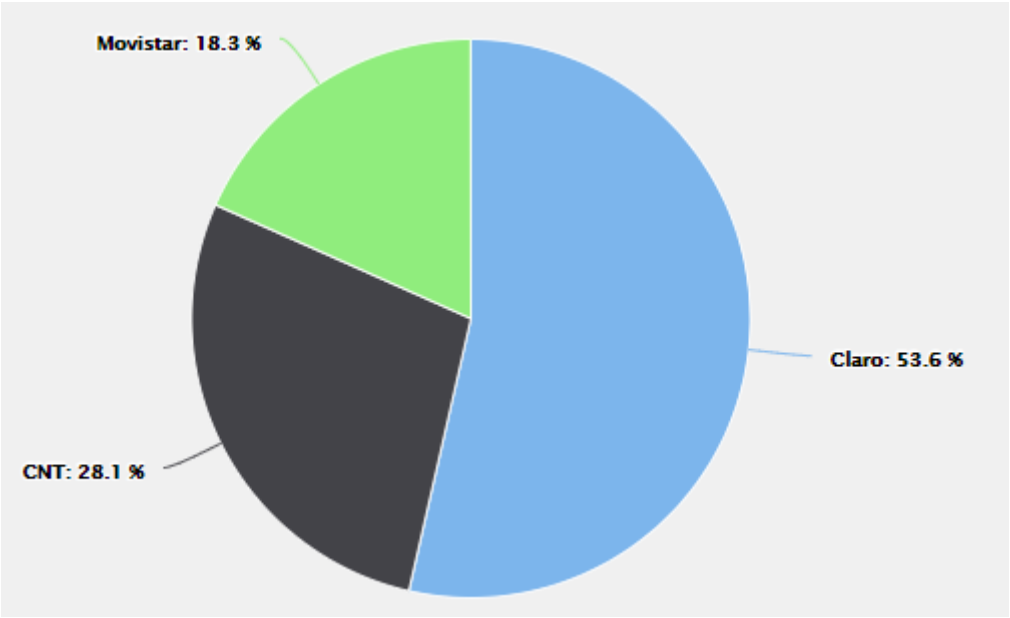


Ilustración 15: Porcentaje de penetración de operadores móviles en el Ecuador
Fuente: [7]

Por lo tanto, se establece que la telefonía móvil más idónea para montar una arquitectura de red sería la de claro, adicionalmente la información adquirida por la aplicación OpenSignal posiciona a claro como una de las operadoras con

mayor número de antenas en la ciudad de Machala tal y como se muestra en la ilustración 16.

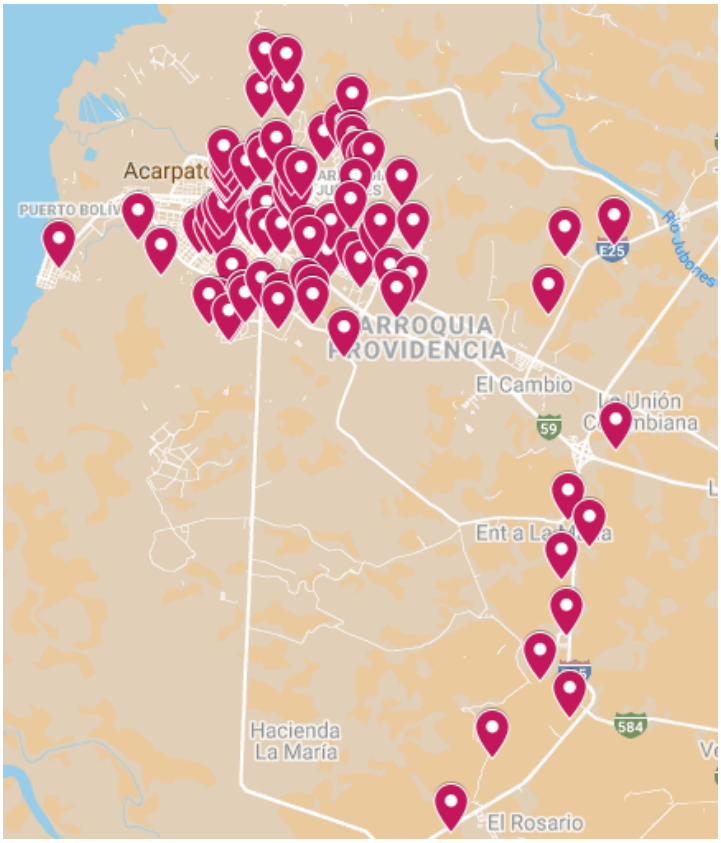


Ilustración 16: Antenas de operadora Claro
Fuente: [8]

Antenas de Operadora Claro

El siguiente cuadro describe las diferentes antenas existentes en la ciudad de Machala de la operadora Claro, en la cual se las ha dividido por parroquia para una mayor compresión de su ubicación, adicionalmente ha sido preseleccionados solo las antenas que cubran las rutas de los buses de la ciudad, con lo cual se podrá tener una mayor apreciación del alcance de la red y analizar si requiere una adquisición de nuevas antenas para extender la red móvil en la trayectoria de la ruta de las diferentes línea de buses.

ANTENAS CLARO			
PARROQUIA	**ANTENA**	**LATITUD**	**LONGITUD**
PUERTO BOLIVAR	PUNTO 1	3.26847	-79.99983
JAMBELI	PUNTO 2	-3.2626	-79.98321
MACHALA	PUNTO 4	-3.26528	-79.97036
	PUNTO 5	-3.26571	-79.96823
	PUNTO 6	-3.26318	-79.96793
	PUNTO 7	-3.26615	-79.96609
	PUNTO 8	-3.26198	-79.96622
	PUNTO 9	-3.26131	-79.96542
JUBONES	PUNTO 24	-3.24602	-79.94449
	PUNTO 25	-3.24362	-79.9409
	PUNTO 26	-3.2381	-79.93865
	PUNTO 27	-3.2454	-79.93868
	PUNTO 28	-3.24652	-79.93857
	PUNTO 29	-3.24957	-79.93746
	PUNTO 30	-3.25104	-79.93629
EL CAMBIO	PUNTO 56	-3.27787	-79.89759
	PUNTO 57	-3.26595	-79.89444
	PUNTO 58	-3.26365	-79.8885
	PUNTO 59	-3.30615	-79.88361
9 DE MAYO	PUNTO 67	-3.27383	-79.96353
	PUNTO 68	-3.28023	-79.96624
	PUNTO 69	-3.28015	-79.96847
	PUNTO 70	-3.28377	-79.96383
	PUNTO 71	-3.27865	-79.9612
	PUNTO 72	-3.27614	-79.97038
	PUNTO 73	-3.27983	-79.9608
	PUNTO 74	-3.27649	-79.95739
EL RETIRO	PUNTO 60	-3.32069	-79.89356
	PUNTO 61	-3.32643	-79.88927
	PUNTO 62	-3.33315	-79.89511
	PUNTO 63	-3.34476	-79.89408
	PUNTO 64	-3.36202	-79.8934
	PUNTO 65	-3.35414	-79.8994
	PUNTO 66	-3.38575	-79.91783
	PUNTO 81	-3.3703	-79.90931
LA PROVIDENCIA	PUNTO 32	-3.25528	-79.93785
	PUNTO 33	-3.25538	-79.92839
	PUNTO 36	-3.26578	-79.95692
	PUNTO 37	-3.2652	-79.95351
	PUNTO 38	-3.25913	-79.95161
	PUNTO 40	-3.25776	-79.95013
	PUNTO 43	-3.26533	-79.94834
	PUNTO 44	-3.27068	-79.9439
	PUNTO 45	-3.2646	-79.94288
	PUNTO 46	-3.26717	-79.94739

	PUNTO 47	-3.26025	-79.93908
	PUNTO 48	-3.27035	-79.93873
	PUNTO 49	-3.2725	-79.9368
	PUNTO 50	-3.26709	-79.93382
	PUNTO 51	-3.26443	-79.93274
	PUNTO 52	-3.26446	-79.92578
	PUNTO 53	-3.27396	-79.93073
	PUNTO 54	-3.27568	-79.9263
	PUNTO 55	-3.2787	-79.92941
	PUNTO 77	-3.27622	-79.94806
	PUNTO 78	-3.27745	-79.94672
	PUNTO 79	-3.28001	-79.94671
	PUNTO 80	-3.28688	-79.9404
	PUNTO 36	-3.3703	-79.90931

Tabla 2: Antenas de Operadora Claro
Fuente: Elaboración Propia

2.4.3. Antenas propuestas para la arquitectura de red

Luego de haber realizado el análisis de las antenas prexistentes de la operadora móvil Claro, se ha propuesto la instalación de nuevas antenas para lograr tener una experiencia de usuario más agradable sin tener que inconvenientes de perdida de señal o desconexión de los equipos que estarán instalado en cada unidad(bus). En la siguiente ilustración se encuentra la distribución por colores de las antenas claro y las nuevas antenas propuestas.

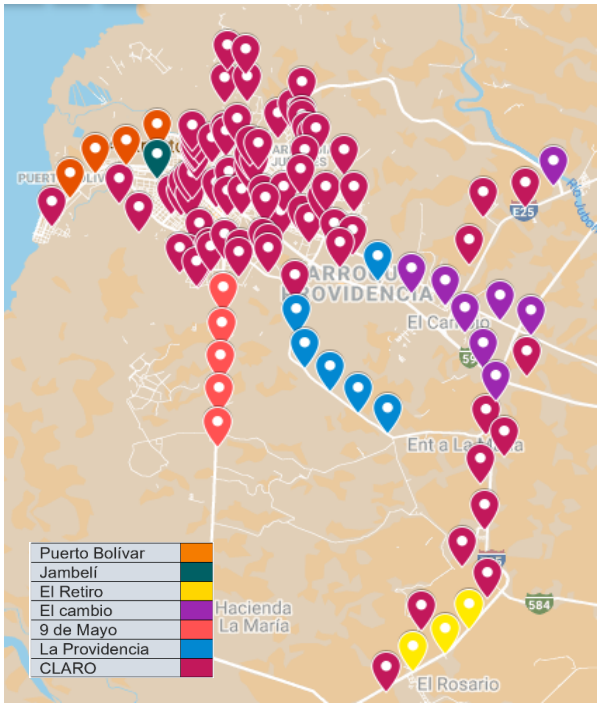


Ilustración 17: Antenas propuestas
Fuente: Elaboración propia

Para complementar y facilitar la ubicación de donde deberían estar instaladas las nuevas antenas de telefonía móvil se ha descrito en la tabla n°3, la ubicación de cada nuevo dispositivo en las diferentes parroquias de la ciudad de Machala junto a su geolocalización.

ANTENAS PROPUESTAS			
PARROQUIA	**ANTENA**	**LATITUD**	**LONGITUD**
PUERTO BOLIVAR	PUNTO 1	3.26847	-79.99983
	ANTENA 1 - PUERTO BOLÍVAR	-3.26431	-79.99826
	ANTENA 2 - PUERTO BOLÍVAR	-3.25891	-79.99323
	ANTENA 3 - PUERTO BOLÍVAR	-3.25334	-79.9866
	ANTENA 4 - PUERTO BOLÍVAR	-3.2533	-79.97786
JAMBELI	PUNTO 2	-3.2626	-79.98321
	ANTENA 1 - JAMBELI	-3.26035	-79.97832
MACHALA	PUNTO 4	-3.26528	-79.97036
	PUNTO 5	-3.26571	-79.96823
	PUNTO 6	-3.26318	-79.96793
	PUNTO 7	-3.26615	-79.96609
	PUNTO 8	-3.26198	-79.96622
	PUNTO 9	-3.26131	-79.96542
JUBONES	PUNTO 24	-3.24602	-79.94449
	PUNTO 25	-3.24362	-79.9409
	PUNTO 26	-3.2381	-79.93865
	PUNTO 27	-3.2454	-79.93868
	PUNTO 28	-3.24652	-79.93857
	PUNTO 29	-3.24957	-79.93746
	PUNTO 30	-3.25104	-79.93629
EL CAMBIO	PUNTO 56	-3.27787	-79.89759
	PUNTO 57	-3.26595	-79.89444
	PUNTO 58	-3.26365	-79.8885
	PUNTO 59	-3.30615	-79.88361
	ANTENA 2 - EL CAMBIO	-3.28861	-79.89707
	ANTENA 4 - EL CAMBIO	-3.29278	-79.8885
	ANTENA 5 - EL CAMBIO	-3.29663	-79.88036
	ANTENA 11 - EL CAMBIO	-3.26126	-79.87694
	ANTENA 13 - EL CAMBIO	-3.29393	-79.90348
	ANTENA 16 - EL CAMBIO	-3.30843	-79.89185
	ANTENA 18 - EL CAMBIO	-3.30843	-79.89185
9 DE MAYO	PUNTO 67	-3.27383	-79.96353
	PUNTO 68	-3.28023	-79.96624
	PUNTO 69	-3.28015	-79.96847
	PUNTO 70	-3.28377	-79.96383
	PUNTO 71	-3.27865	-79.9612
	PUNTO 72	-3.27614	-79.97038
	PUNTO 73	-3.27983	-79.9608
	PUNTO 74	-3.27649	-79.95739

	ANTENA 6 - MACHALA	-3.2903	-79.95779
	ANTENA 9 - MACHALA	-3.299	-79.95805
	ANTENA 10 - MACHALA	-3.3065	-79.95843
	ANTENA 11 - MACHALA	-3.31529	-79.95881
	ANTENA 12 - MACHALA	-3.32415	79.95926
EL RETIRO	PUNTO 60	-3.32069	-79.89356
	PUNTO 61	-3.32643	-79.88927
	PUNTO 62	-3.33315	-79.89511
	PUNTO 63	-3.34476	-79.89408
	PUNTO 64	-3.36202	-79.8934
	PUNTO 65	-3.35414	-79.8994
	PUNTO 66	-3.38575	-79.91783
	PUNTO 81	-3.3703	-79.90931
LA PROVIDENCIA	PUNTO 32	-3.25528	-79.93785
	PUNTO 33	-3.25538	-79.92839
	PUNTO 36	-3.26578	-79.95692
	PUNTO 37	-3.2652	-79.95351
	PUNTO 38	-3.25913	-79.95161
	PUNTO 40	-3.25776	-79.95013
	PUNTO 43	-3.26533	-79.94834
	PUNTO 44	-3.27068	-79.9439
	PUNTO 45	-3.2646	-79.94288
	PUNTO 46	-3.26717	-79.94739
	PUNTO 47	-3.26025	-79.93908
	PUNTO 48	-3.27035	-79.93873
	PUNTO 49	-3.2725	-79.9368
	PUNTO 50	-3.26709	-79.93382
	PUNTO 51	-3.26443	-79.93274
	PUNTO 52	-3.26446	-79.92578
	PUNTO 53	-3.27396	-79.93073
	PUNTO 54	-3.27568	-79.9263
	PUNTO 55	-3.2787	-79.92941
	PUNTO 77	-3.27622	-79.94806
	PUNTO 78	-3.27745	-79.94672
	PUNTO 79	-3.28001	-79.94671
	PUNTO 80	-3.28688	-79.9404
	PUNTO 36	-3.3703	-79.90931
	ANTENA 1 - LA PROVIDENCIA	-3.31824	-79.92038
	ANTENA 2 - LA PROVIDENCIA	-3.3125	-79.92793
	ANTENA 3 - LA PROVIDENCIA	-3.30739	-79.93462
	ANTENA 4 - LA PROVIDENCIA	-3.30109	-79.94102
	ANTENA 5 - LA PROVIDENCIA	-3.29252	-79.93891
	ANTENA 24 - LA PROVIDENCIA	-3.28088	-79.93041

Tabla 3: Antenas propuestas
Fuente: Elaboración propia

2.4.4. Red móvil

Los datos estadísticos de la Arcotel [46], que es el organismo que regula las telecomunicaciones y el espectro radioeléctrico del País, indica la evolución de las diferentes redes móviles existente desde el 2010 hasta el 2019, en el cual se logra observa como la tecnología LTE ha ido creciendo posicionándose con cerca del 50% con respecto a la tecnología 2G y 3G. Existe una nueva generación de red móvil la cual es la 5G con velocidades de hasta 10Gbps pero al ser una tecnología relativamente nueva aún no tiene un impacto tan grande dentro del territorio ecuatoriano.

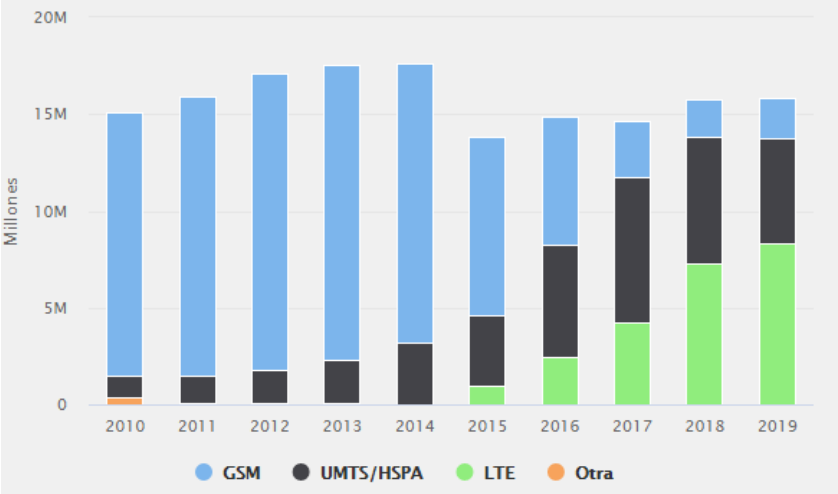


Ilustración 18: Evolución de generaciones móviles en Ecuador
Fuente: [7]

La tecnología 4G también llamada LTE ha predominado el mercado debido a las nuevas prestaciones que suministra al usuario tanto una velocidad mejorada y cobertura con respecto a sus predecesoras con lo que mejora mucho la calidad con la que el usuario interactúa con ella, en cuanto a lo que se refiere las antiguas generaciones como la 2G y 3G no se encuentra en un total desuso, sino que se las usa como redes complementaria dentro de la misma telefonía para lograr obtener una conexión casi continua.

2.5. Ejecución y/o ensamblaje del prototipo

Para la implementación de la arquitectura de red propuesta, primero se debe considerar la seguridad de la misma aplicando la Normativa ISO/IEC 27033, la cual establece la gestión de seguridad en la administración, operación y uso de la red a diseñar [47]. Además, se debe seguir el modelo PHVA, en donde debe existir una planificación para verificar el estado actual de la red, y con ello realizar

los cambios respectivos no definitivos para implementar las pruebas correspondientes, siguiendo con la verificación de los mismos hasta culminar con el desarrollo.

Según la normativa se debe seguir 6 procesos para asegurar que la implementación sea segura y mitigar los posibles riesgos que puedan ocurrir. Antes de incurrir a dichos procesos se describen los activos que conforman la arquitectura de red y a partir de ellos identificar los riesgos y amenazas que podrían ocasionar fallos en producción.

2.5.1. Descripción de activos y equipos

Activo	Cantidad	Descripción
Nokia Flexi Multiradio BTS	23	eNodeB, Sera el encargado de dirigir las comunicaciones tanto en la transmisión y recepción de los diferentes dispositivos que se conecten a la misma.
Flexi NS	2	MME, la función que realiza primordialmente es la de proporcionar funcionalidades de control sobre la red EPC.
Flexi NG	2	(S-GW & P-GW), suministran de conectividad al usuario con la red de radio acceso y redes datos externas como el internet.
Interface S1	1	Permite la comunicación entre E-UTRAN y EPC
Interface X2	1	Permite la interconexión de los diferentes eNodeB, además reduce las interferencia
Interface S5	1	Es la interfaz lógica que conecta el SWG con PGW
Interface S6a	1	Es una interfaz lógica que permite la comunicación entre MME y HSS
S11	1	Es utilizada comúnmente para conectar vía túnel a SGW con la MME

Interface de radio Uu		Realiza la comunicación entre el UE con las terminales de tipo eNodeB.
Interfaz SGi		Conecta a las redes de datos externas (IMS o Internet) con la P-GW, transportando datos en protocolos IPv4 así como también protocolos IPv6.

Tabla 4: Descripción de activos
Fuente: Elaboración propia

Los elementos utilizados para el montaje de la infraestructura de la red será de la marca Nokia tanto en hardware y software, la instalación de cada dispositivo se lo realizará en los puntos GPS indicados en la tabla N°4, para complementar las estaciones bases ya instaladas por la operadora, pero manteniendo las normas establecidas por la ISO 27033 y brindar tanto un servicio estable y seguro durante todo el trayecto de las rutas de buses.

2.5.2. ISO/IEC 27033-1 Visión General y conceptos

Tipos de seguridad

Seguridad Física

La seguridad física es aquella que trata de proteger el hardware (los equipos informáticos, el cableado, equipos de red, etc.) de los posibles desastres naturales (terremotos, huracanes, etc.), incendios, inundaciones, sobrecargas eléctricas, robos y un sinfín de amenazas más.

Seguridad Lógica

Esta seguridad es un complemento de la seguridad física, comprende la protección del software de los dispositivos informáticos, como son las aplicaciones, información del usuario, fallos en conexión, código malicioso, accesos no autorizados a la información, en fin, todos los posibles ataques que puedan surgir físicamente en los componentes de la red.

Seguridad Activa

Son el grupo de medidas que permiten mitigar los daños causados por software malicioso.

Seguridad Pasiva

Este tipo de seguridad es un complemento a la seguridad activa la cual se encarga de la minimización de riesgos que surjan de los ataques a los dispositivos de conexión ocasionando distintos percances.

Tipos de amenazas

Amenazas naturales

Estas amenazas son todos aquellos desastres naturales en los cuales no se tiene un control sobre ellos como: incendios, inundaciones, terremotos, etc. Muchas empresas no inventen tanto en ese tipo de amenazas, a menos que su ocurrencia sea inminente. Sin embargo, deben estar consideradas en un plan de contingencias.

Amenazas físicas

Son aquellas amenazas que no se siente físicamente su daño sino más bien atacan el sistema lógico informático, suelen ser programas infectados con malware, bugs o exploits que comprometen al sistema operativo y éste queda expuesto a irrupciones o también a fallos.

Ataques Genéricos

Son el conjunto de debilidades existente en los diferentes sistemas informáticos que permiten que los vulneren.

2.5.2.1. Establecimiento de políticas

Políticas	Descripción
Política de asignación y etiquetado de equipos.	Los equipos deben estar etiquetados, para que en caso de presentar fallas o daños sea más fácil realizar una restauración.
Política de seguridad física y del entorno	Definir un listado de acceso a los dispositivos, solo al personal autorizado
Política de protección contra amenazas externas y ambientales	Todos los equipos deben estar protegidos sobre fallas de energía. Proveer un respaldo de la información e inventario de los dispositivos, además de contar con un plan de contingencia

Política de ubicación y protección de los equipos	Ubicar a los equipos en lugares seguros y fuera del alcance de personal no autorizado.
Política de controles físicos de entrada	Todo el personal debe tener una identificación para ingresar a las instalaciones.
Políticas de seguridad de los recursos humanos	El personal debe conocer los estatutos de la empresa.
Políticas relacionada con la desvinculación y cambios de labores	El personal debe firmar un contrato de confidencialidad sobre toda la información que maneje.
Políticas de administración de activos de la red	El personal debe conocer y desempeñar sus funciones según corresponda el rol que se le asignó.
Política de protección frente a software malicioso	El sistema debe contar con un plan de corrección y mantenimiento de código malicioso, además de tener actualizaciones periódicamente.
Política de control de acceso	Lineamientos para el acceso a la información según el rol asignado.
Política de Gestión de red	Debe existir una comunicación en la gestión de redes.

Tabla 5: Establecimiento de políticas
Fuente: Elaboración propia

En base a estas definiciones la normativa ISO/IEC 27033-1 plantea los siguientes controles para asegurar la seguridad de la red.

Control		Tipo
Actividades de gestión de la seguridad de la red	Una política de seguridad documentado con arquitectura de seguridad técnica adjunta.	Lógica
	Realice comprobaciones de seguridad para garantizar que las medidas implementadas fueron suficiente.	Física
	Documentar las condiciones que deben cumplirse en la red antes de realizarse una conexión.	Lógica

	Las condiciones de seguridad necesarias para usuarios remotos.	Lógica
	Plan de emergencia	Lógica
Responsabilidades	División de responsabilidades para reforzar la seguridad de la red de una organización.	Física
Política de Seguridad de la red	Ocuparse específicamente de los requisitos de seguridad de la red para el uso de los recursos, servicios y aplicaciones que deben estar presentes.	Física
SecOps red	Describir el apoyo que debe recibir la política de seguridad de los operadores o actores involucrados en las operaciones diarias. Estos documentos incluyen la asignación de responsabilidades.	Lógica
Verificación de las Correcciones en la seguridad de la red	Testear la eficiencia de las medidas para el mantenimiento y la mejora continua de la seguridad de la información.	Lógica
Las condiciones de seguridad para las conexiones de red	La transferencia de información a otros puntos finales (por ejemplo, internet) posee el riesgo que en el otro extremo de la comunicación no se implementen los requisitos para la seguridad de su propia organización.	Física
Las condiciones de seguridad documentados para usuarios remotos	Documentar las políticas de seguridad para el uso de las VPN.	Lógica

Tabla 6: Controles ISO/IEC 27033-1
Fuente: [48]

2.5.3. ISO/IEC 27033-2 Directrices para el diseño e implementación de la seguridad de la red

Para realizar un diseño de red seguro, destacamos las siguientes directrices:

- Analizar la ubicación geográfica de donde se realizará la implementación infraestructura de red.
- Identificar las zonas de menos cobertura.
- Identificar cual es la operadora móvil más idónea para iniciar con el proyecto.
- Adquirir los equipos con mayor índice de durabilidad.
- Seguir las normas para una buena implementación de seguridad en la red.

- Identificar los riesgos que se puede presentar durante la implementación de la red.
- Definir controles.

2.5.4. ISO/IEC 27033-3 Escenarios de riesgos – amenazas, técnicas de diseño y problemas

Identificación de amenazas

Actualmente un sistema de transporte urbano, presenta muchas vulnerabilidades con respecto a la seguridad de sus equipos, ya sea por accidentes de tránsito o por sustracción de los dispositivos.

A continuación, se presenta una lista de las amenazas más comunes que se podrían presentar en la implementación de la arquitectura de red para un sistema de buses inteligentes.

- Tragedias naturales.
- Interrupción en la alimentación del equipo instalado en el autobús.
- Fallos de software en los dispositivos de red.
- Fallos de hardware en los componentes de red.
- Interrupciones de conectividad de internet.
- Desconocimiento en el manejo del software.
- Desconexión en la base datos (pérdida de registros).

Gestión de riesgos

Daños en los equipos de conectividad: fallos en la manipulación de dispositivos, como el módulo de control o GPS dentro del bus, o también equipos como MME que se encuentran externos al autobús.

Tragedias naturales: Fuertes lluvias podrían ocasionar que alguna antena colapse y se pierda conectividad.

Irrupción a los activos: Usuarios mal intencionados puedan hurtar la información proporcionada en la red.

Interrupción en la alimentación de energía: Las antenas pueden quedarse sin batería para alimentar a sus dispositivos internos, y a su vez perder la conexión a internet.

Suplantación de identidad: personas ajenas a las actividades operativas de la red, puedan acceder a la información.

Finalizar contratos de trabajos en malos términos: culminación de contratos o cambio de cargos en el equipo de trabajo que operan la red.

Inadecuado uso de permisos de usuario: personas que por error o conscientemente realicen actividades ajenas a su cargo.

Código malicioso: propagación de código mal intencionado por parte de terceros hacia la red.

Acceso por entidades externas al servidor: acceso a la información privada o sensible de la red que se encuentra en servidores.

Congestión en la red: gran cantidad de usuarios conectados a la vez a la red.

2.5.5. ISO/IEC 27033-4 Protección de las comunicaciones entre redes mediante pasarelas de seguridad.

Para realizar este proceso la normativa ofrece anexos que ayudan a la implementación de los mismo, según nuestra arquitectura se ha elegido el anexo A.2 y A.6 los cuales abarcan los controles sobre las redes de área amplia y Gateways de seguridad.

A.2 Redes de Área amplia	
1	Reemplazo de los protocolos muy inseguros como Telnet y FTP por SSH o TFTP.
2	El cifrado del tráfico de red.
3	Ejecutar alertas de SNMP para la autenticación segura en el acceso a los equipos WAN.
4	Efectuar vías de contingencia en las entradas y salidas de consultas.
5	Asignar equipos de red para la identificación de equipos no autorizados en la red.
6	Obtener garantías del proveedor de servicios que mitiguen la latencia y jitter en sus conexiones.
7	Implementación de auditoría para el acceso a los dispositivos WAN.
8	Uso de firewall para identificar el tráfico no deseado que ingresa a la red.
9	Uso de sistemas especializados en la evitación de código malicioso tales como malware, troyanos, virus, gusanos, spyware, entre otros.

10	Usar IDS para determinar el tráfico malicioso dentro de la red.
11	Afirmar los sitios de gestión de redes físicamente seguros.
12	Afirmar que los equipos de red tienen respaldos.

Tabla 7: Anexo A.2 Redes de área amplia
Fuente: [48]

A.6 Gateways de Seguridad	
1	Disociación virtual de la red.
2	Suministrar puntos únicos controlados y manejo de flujos de entrada a la red.
3	Cumplir con las políticas de seguridad de la organización en cuanto a las conexiones de red
4	Suministrar puntos únicos de acceso para que los operadores registren el ingreso.

Tabla 8: Anexo A.6 Gateways de Seguridad
Fuente: [48]

2.5.6. ISO/IEC 27033-5 Protección de las comunicaciones a través de redes mediante redes privadas virtuales

Para la arquitectura de red diseñada, los usuarios finales se conectan mediante el protocolo GTP-U, el cual se basa en el tunelamiento GPRS, que se encarga de facilitar la movilidad dentro de las redes 3GPP, este protocolo encapsula e incluye en la cabecera de cada paquete IP el identificador del túnel por el cual va a pasar, su longitud y el número de secuencia.

2.5.7. ISO/IEC 27033-6 Asegurar el acceso a la red IP Inalámbrica

Este proceso se lo realiza teniendo un registro de todos los usuarios con sus permisos y credenciales correspondientes para que tengan acceso a los módulos y equipos determinados.

La red LTE4G, según [49] ofrece tres tipos básicos de bloques de seguridad:

- Autenticación LTE: este tipo de autenticación es el proceso en donde se determina si un usuario es está autorizado para acceder a la red.
- Seguridad NAS (Estrato sin acceso): son mecanismos indispensables para otorgar de forma íntegra los paquetes NAS receptados por los usuarios finales y un MME.
- Seguridad AS (Estrato de acceso): se refiere a los componentes necesarios para otorgar de forma íntegra los paquetes AS receptados por los usuarios finales y un eNodeB:

Para ejecutar una autenticación recíproca en una red LTE se utilizan EPS con autenticación y acuerdo de claves, estos constan de dos pasos:

1. Un HSS genera uno o varios vectores de autenticación del tipo: RAND, AUTN, XRES, KASME y los entrega al MME que está en inmediación con los usuarios finales.

2. El MME elige uno de los vectores de autenticación, lo usa para la autenticación mutua con el UE y para compartir una clave de autenticación (KASME).

La red tiene que ser verificada porque los usuarios pueden estar en roaming.

2.5.8. Gestión de Controles

Para realizar la gestión de controles se debe considerar una metodología para analizar los riesgos que se puedan presentar en la implementación de la arquitectura de red, este análisis se realizará por colores de manera cualitativa con la finalidad de establecer los niveles de riesgos mediante la combinación de los códigos de colores y una ponderación de 0,0 al 3,0 dependiendo del nivel de riesgo.

Evento	Descripción	Color
Posible	Aquel fenómeno que se puede presentar porque no existen hechos históricos para afirmar que no sucederá.	Verde
Probable	Aquel fenómeno que se espera porque existen razones previas de científicos que creen que sucederá.	Amarillo
Inminente	Aquel fenómeno que se espera porque tiene gran probabilidad de que suceda.	Rojo

Tabla 9: Definición de metodología
Fuente: [45]

En la calificación según el nivel de riesgo se considera tres estados, el primer nivel está en un rango entre 0 a 1 con color verde en una frecuencia que indica que jamás ha sucedido, el segundo nivel entre un rango de 1 a 2 se representa con color amarillo se encuentra en frecuencia que ya ha sucedido, mientras que

el último nivel está entre el rango de 2 a 3 e indica la frecuencia que es evidente y detectable representado con color rojo.

Rango	Calificación	Frecuencia	Color
0,0 – 1,0	Baja	Jamás ha sucedido	Verde
1,1 – 2,0	Media	Ya ha sucedido	Amarillo
2,1 – 3,0	Alta	Evidente, detectable	Rojo

Tabla 10: Calificación según colores
Fuente: [45]

Para la valorización de los activos en cambio tendrán valores a partir de criterios de Confidencialidad, Integridad y Disponibilidad, los cuales van a tener una ponderación de 1 a 3 dependiendo de su nivel de influencia, siendo bajo desde 0,1 a 1,0, medio de 1,1 a 2,0 y crítico de 2,1 a 3,0.

Valor	Descripción	Confidencialidad	Integridad	Disponibilidad
1	Bajo	El activo puede ser accedido por todos.	Las configuraciones iniciales pueden ser alteradas.	El Activo no siempre puede estar disponible.
2	Medio	El activo solo puede ser accedido mediante autorización.	Las configuraciones iniciales solo pueden ser alteradas mediante autorización.	El activo puede o no, estar disponible
3	Crítico	El activo no puede ser accedido, solamente los operadores responsables pueden acceder.	Las configuraciones iniciales no pueden ser alteradas, solamente los operadores responsables pueden realizar cambios.	El activo debe estar disponible siempre.

Tabla 11: Valor del Activo
Fuente: Elaboración propia, basada en [47]

En base a esta calificación la fórmula para encontrar el valor sería:

$$Valor\ Activo = \frac{Confidencialidad + Integridad + Disponibilidad}{3}$$

Información del Riesgo				Ubicación	
Riesgo	Fuente del riesgo	Calificación	Color	Interno	Externo
Conexión en equipos de conectividad	Daños en los equipos de conectividad.	1,5	Amarillo	x	x
Acceso a los dispositivos	Fallos en la manipulación de dispositivos, como el módulo de control o gps dentro del bus, o también equipos como MME que se encuentran externos al autobús.	1,0	Verde	x	x
Desastres naturales	Fuertes lluvias podrían ocasionar que alguna antena colapse y se pierda conectividad.	1,5	Amarillo	x	x
Irrupción a los activos	Usuarios mal intencionados puedan hurtar la información proporcionada en la red.	1,7	Amarillo	x	x
Interrupción en la alimentación de energía	Las antenas pueden quedarse sin batería para alimentar a sus dispositivos internos, y a su vez perder la conexión a internet.	3,0	Rojo	x	x
Suplantación de identidad	Personas ajenas a las actividades operativas de la red, puedan acceder a la información.	0,5	Verde	x	
Contratos de trabajos	Culminación de contratos o cambio de cargos en el equipo de trabajo que operan la red.	0,5	Verde	x	
Termino o cambio de contrato	Cambio de cargos en el equipo de trabajo.	0,5	Verde	x	
Permisos de usuario	Personas que por error o conscientemente realicen actividades ajenas a su cargo.	3,0	Rojo	x	
Código malicioso	Propagación de código mal intencionado por parte de terceros hacia la red.	1,8	Amarillo	x	
Acceso por entidades externas al servidor	Acceso a la información privada o sensible de la red que se encuentra en servidores.	3,0	Rojo		x
Congestión en la red	Gran cantidad de usuarios conectados a la vez a la red.	0,9	Verde	x	x

Tabla 12: Matriz de riesgos
Fuente: Elaboración propia

La ISO/IEC 27033 establece que también sean evaluados los activos que intervienen en la red por lo cual aplicaremos la misma metodología aplicada anteriormente con los colores verde, amarillo y rojo para definir el nivel de riesgo.

	Información del activo			Clasificación de activos				Ubicación	
#	Tipo	Activo	Descripción	C	I	D	Valor	Interno	Externo
1	Hardware	Nokia Flexi Multiradio BTS	eNodeB, Sera el encargado de dirigir las comunicaciones tanto en la transmisión y recepción de los diferentes dispositivos que se conecten a la misma.	1	2	3	2		x
2	Hardware	Flexi NS	MME, la función que realiza primordialmente es la de proporcionar funcionalidades de control sobre la red EPC.	3	3	3	3	x	
3	Hardware	Flexi NG	(S-GW & P-GW), suministran de conectividad al usuario con la red de radio acceso y redes datos externas como el internet.	1	1	3	2	x	
4	Servicios	Interface S1	Permite la comunicación entre E-UTRAN y EPC	3	3	3	3		x
5	Servicios	Interface X2	Permite la interconexión de los diferentes eNodeB, además reduce las interferencia	1	1	1	1		x
6	Servicios	Interface S5	Es la interfaz lógica que conecta el SWG con PGW	3	3	3	3	x	
7	Servicios	Interface S6a	Es una interfaz lógica que permite la comunicación entre MME y HSS	3	3	3	3	x	
8	Servicios	S11	Es utilizada comúnmente para conectar vía túnel a SGW con la MME	3	3	3	3	x	
9	Servicios	Interface de radio Uu	Realiza la comunicación entre el UE con las terminales de tipo eNodeB.	2	3	3	3		x
10	Servicios	Interfaz SGi	Conecta a las redes de datos externas (IMS o Internet) con la P-GW, transportando datos en protocolos IPv4, así como también protocolos IPv6.	3	3	3	3		x

Tabla 13: Matriz de riesgos de los activos
Fuente: Elaboración propia

2.5.9. Análisis de Riesgos

A partir de la matriz de riesgo detallada en el punto anterior se puede obtener el siguiente análisis:

- Conexión en equipos de conectividad, daño en los equipos que pueden ser resultados de la interrupción de red, se considera un riesgo de carácter interno como externo, con un nivel medio de riesgo e identificado de color amarillo.
- Acceso a los dispositivos, puede ser ocasionado por fallos en la manipulación de dispositivos, calificado de carácter interno y externo con un nivel de riesgo bajo e identificado de color verde.
- Desastres naturales, considerado de carácter interno y externo con un nivel de riesgo medio, los cuales pueden ocurrir en cualquier momento y ocasionar daño en todo tipo de equipos.
- Irrupción a los activos, sucede cuando las personas con actitudes delictivas roban información de la red con intensión de extorsión o fines lucrativos, calificado de carácter interno y externo, con un nivel de riesgo medio.
- Interrupción en la alimentación de energía eléctrica, puede suscitarse en la baja de suministro eléctrico ocasionando daño en los equipos, este riesgo es considerado con un nivel alto de color rojo, con carácter interno y externo.
- Suplantación de identidad, personas ajenas al funcionamiento de la red que puedan acceder a las cuentas de los usuarios, calificado de carácter interno con un nivel bajo de riesgo.
- Contratos de trabajo, se puede presentar porque el personal puede incurrir en actos ilícitos que provoquen errores o pérdidas de información, considerado de carácter interno con un nivel de riesgo bajo.
- Termino o cambio de contrato, puede suscitarse que el personal despedido pueda revelar información comprometida de la red, con un nivel de riesgo bajo, calificada de carácter interno.
- Permisos de usuario, puede presentarse cuando el personal realice actividades que no competen a su cargo, con un nivel de riesgo alto de carácter interno.

A continuación, se detalla los controles que se llevarán a cabo a partir de los riesgos analizados con anterioridad.

Políticas	Controles	Descripción
Política de asignación y etiquetado de equipos.	Conexión en equipos de conectividad	La conexión debería estar protegida contra interrupciones o daños.
Política de seguridad física y del entorno	Acceso a los dispositivos	Definir una política de control de acceso a los dispositivos, solo al personal autorizado
Política de protección contra amenazas externas y ambientales	Desastres naturales	Tener respaldo de la información y tener en inventario todos los dispositivos. Además de contar con un plan de contingencia
Política de protección contra amenazas externas y ambientales	Interrupción en la alimentación de energía	Los equipos deben protegerse sobre fallas de energía. Contar con un generador o regulador de energía.
Política de ubicación y protección de los equipos	Irrupción a los activos	Definir políticas para la seguridad de la información. Además de asignar responsabilidades de esta seguridad para esta información.
Política de controles físicos de entrada	Suplantación de identidad	Definir una política de control de acceso como tarjetas de identificación para cada persona de la empresa.
Políticas de seguridad de los recursos humanos	Contratos de trabajos	Asegurarse que los empleados conozcan las responsabilidad y roles que tienen en la empresa.

Políticas relacionada con la desvinculación y cambios de labores	Termino o cambio de contrato	Definir una política de confidencialidad sobre la información. Además de comunicar el despido o cambio del personal.
Políticas de administración de activos de la red	Permisos de usuario	Definir y asignar los roles y permisos para cada persona de la empresa.
Política de protección frente a software malicioso	Código malicioso	Instalar software que detecte código malicioso, como antivirus y tenerlo actualizado
Política de control de acceso	Acceso por entidades externas al servidor	Implementar un Sistema de Detección de Intrusos para identificar el tráfico sospechoso dentro de la red
Política de Gestión de red	Congestión en la red	Implementar en un sistema de conmutación para facilitar el manejo de tráfico de la red.

Tabla 14: Listado de controles
Fuente: Elaboración propia

3. CAPÍTULO III. EVALUACIÓN DEL PROTOTIPO

3.1. Plan de evaluación

Para realizar el plan de evaluación de la arquitectura de red propuesta, se realiza un cuestionario para verificar si cumple con los controles descritos en el capítulo anterior, se ha tomado como referencia el plan de evaluación del autor [50].

DESCRIPCIÓN	RESPUESTAS		Porcentaje
	SI	NO	
Seguridad Física			
Uso adecuado de los activos	x		100%
Gestión de los recursos tecnológicos	x		100%
Control de acceso físico	x		100%
Protección y ubicación de los equipos	x		100%
Gestión de medios removibles		x	0%
Riesgos relacionados con terceros.	x		100%
Seguridad lógica			
Control de acceso lógico	x		100%
Definición de roles de usuario	x		100%
Protección contra software malicioso	x		100%
Copias de respaldo	x		100%
Seguridad para el intercambio de información	x		100%
Gestión de contraseñas de usuario	x		100%
Escritorio y pantalla limpia		x	0%
Seguridad ligada al personal			
Acuerdos de confidencialidad	x		100%
Gestión del talento Humano		x	0%
Culminación o cambio de contrato laboral	x		100%
Comunicación y operaciones			
Acceso a internet	x		100%
Segregación de redes	x		100%

Tabla 15: Plan de Evaluación
Fuente: Elaboración propia, basada en [50]

3.2. Resultados de la evaluación

Una vez realizado el plan de evaluación, se realiza el análisis de resultados, en donde se destacan los controles que se deben trabajar: en la seguridad física, la gestión de medios removibles no se cumple al 100% debido a que no se permite la conexión de dispositivos físicos removibles a la red. En la seguridad lógica en cambio el control que no se cumple al 100% es el de Escritorio y pantalla limpia, debido a que no existe un acceso con interfaz de usuario sino más bien de tipo terminal, este control no aplica dentro de nuestra arquitectura de red. Mientras que la gestión de talento humano no se cumple ya que no existe un plan de cómo elegir al personal cualificado para desempeñar sus funciones, debido a que son dispositivos con configuraciones propias del sistema que solo pueden ser manipuladas por personal autorizado

3.3. Conclusiones

En base al trabajo realizado se puede sacar las siguientes conclusiones:

- Se diseñó una arquitectura de red mediante la ISO 27033 para un sistema de buses inteligentes en la ciudad de Machala.
- Para el análisis de la información se investigó en su mayoría en fuentes bibliográficas científicas en base a los últimos 5 años. Además, se trabajó con la herramienta Mendeley para el almacenamiento de la información bibliográfica.
- Una vez identificadas las tecnologías inalámbricas se trabajó en base a la tecnología 4G LTE, ya que se destaca de las demás por su mayor cobertura.
- Se trabajó la infraestructura de nuestra propuesta en base a la tecnología 4G y las antenas telefónicas de Claro para el diseño de la arquitectura de red para la ciudad de Machala.

3.4. Recomendaciones

- Adicionalmente de la implementación de la arquitectura bajo los parámetros de la norma ISO 27033 se recomienda tener un plan de mantenimiento semestral de los equipos para asegurar la calidad del servicio.

- Se recomienda utilizar la herramienta Mendeley, para realizar la bibliografía del documento, ya que facilito la obtención de la información de los autores y su trabajo.
- Una de las mejores opciones es utilizar la tecnología 4G debido a que se encuentra en su auge, con lo cual las operadoras móviles realizan constantemente mantenimiento e instalaciones de nuevos equipos, ampliando aún más su cobertura.
- Se recomienda que para elección de la infraestructura y de la operadora móvil se realice un estudio del territorio en donde se vaya a realizar la instalación de nuevos equipos, ya que dependiendo de la operadora esto puede variar.

4. BIBLIOGRAFÍA

[1] J. Jimenez, “Smart Transportation Systems,” *Smart Cities*, pp. 123–133, 2017, doi: https://doi.org/10.1007/978-3-319-59381-4_8.

[2] A. J. Kadam, V. Patil, K. Kaith, D. Patil, and Sham, “Developing a Smart Bus for Smart City using IOT Technology,” *Proc. 2nd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2018*, no. Iceca, pp. 1138–1143, 2018, doi: 10.1109/ICECA.2018.8474819.

[3] ISO27001, “ISO 27001 - Software ISO 27001 de Sistemas de Gestión.” https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (accessed Apr. 07, 2021).

[4] M. Cello, C. Degano, M. Marchese, and F. Podda, *Smart transportation systems (STSs) in critical conditions*. Elsevier Inc., 2016.

[5] M. Gohar, M. Muzammal, and A. Ur Rahman, “SMART TSS: Defining transportation system behavior using big data analytics in smart cities,” *Sustain. Cities Soc.*, vol. 41, pp. 114–119, 2018, doi: 10.1016/j.scs.2018.05.008.

[6] EPMMM, “Empresa Pública Municipal Movilidad Machala,” 2021. http://www.movilidadmachala.gob.ec.

[7] TeleSemana, “Estadísticas: telecomunicaciones en Ecuador – TeleSemana.com.” https://www.telesemana.com/panorama-de-mercado/ecuador/ (accessed Apr. 09, 2021).

[8] OpenSignal, “Mobile Analytics & Insights | Opensignal.” https://www.opensignal.com/ (accessed Apr. 09, 2021).

[9] L. Fedele and L. Fedele, “From Basic Maintenance to Advanced Maintenance,” *Methodol. Tech. Adv. Maint.*, pp. 63–112, 2011, doi: 10.1007/978-0-85729-103-5_5.

[10] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A Literature Review,” *J. Comput. Commun.*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.

[11] V. Alvear, “Internet de las Cosas y Visión Artificial, Funcionamiento y

Aplicaciones: Revisión de Literatura (Internet of Things and Artificial Vision, Performance and Applications: Literature Review)," *Enfoque UTE*, vol. 8, no. 1, pp. 244–256, 2017, [Online]. Available: http://ingenieria.ute.edu.ec/enfoqueute/.

[12] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, no. March, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.

[13] B. Clara, R. Damer, and D. Beatrice Paola, "Smart Mobility in Smart City," *Empower. Organ.*, vol. 11, pp. 13–28, 2016, doi: https://doi.org/10.1007/978-3-319-23784-8_2.

[14] T. hoon Kim, C. Ramos, and S. Mohammed, "Smart City and IoT," *Future Generation Computer Systems*, vol. 76. Elsevier B.V., pp. 159–162, Nov. 01, 2017, doi: 10.1016/j.future.2017.03.034.

[15] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Commun. Mag.*, vol. 55, pp. 122–129, 2017, doi: 10.1109/MCOM.2017.1600267CM.

[16] B. Muhammad and F. Arif, "Real-time data processing scheme using big data analytics in internet of things based smart transportation environment," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, pp. 4167–4177, 2019, doi: https://doi.org/10.1007/s12652-018-0820-5.

[17] M. Aamir, S. Masroor, Z. A. Ali, and B. T. Ting, "Sustainable Framework for Smart Transportation System: A Case Study of Karachi," *Wirel. Pers. Commun.*, vol. 106, no. 1, pp. 27–40, 2019, doi: 10.1007/s11277-019-06259-4.

[18] Z. Karami and R. Kashef, "Smart transportation planning: Data, models, and algorithms," *Transportation Engineering*, vol. 2. p. 100013, 2020, doi: 10.1016/j.treng.2020.100013.

[19] P. Alvarado Medellin, S. P. Aguilar Escarcia, A. M. Ramírez Aguilrera, and R. Ortiz Gómez, "Dynamic system for monitoring and control wireless sensor networks operating under ZigBee comunication protocol," *Ing.*

Investig. y Tecnol., vol. 20, no. 1, pp. 1–9, 2019, doi: 10.22201/fi.25940732e.2019.20n1.003.

[20] C. R. Egas, D. Viracocha, and J. Rivera, “Implementación de una red inalámbrica de sensores para la gestión de luminarias utilizando IPv6,” *Enfoque UTE*, vol. 10, no. 4, pp. 45–56, 2019, doi: 10.29019/enfoque.v10n4.553.

[21] CNMC, “Redes WiMAX y wifi,” *CNMC*, 2019. https://blog.cnmc.es/2010/05/28/conceptos-basicos-de-telecos-redes-inalambricas-fijas-y-en-bandas-de-uso-comun/ (accessed Apr. 09, 2021).

[22] A. Gawanmeh and Y. Iraqi, “Formal analysis of collision prevention of two wireless personal area networks,” *Procedia Comput. Sci.*, vol. 80, pp. 2362–2366, 2016, doi: 10.1016/j.procs.2016.05.443.

[23] T. CÉSAR, “Evaluación De Tecnologías Inalámbricas En Redes De Área Doméstica Para Obtener La Curva Característica De Carga En Edificios Inteligentes.,” 2019.

[24] Cámara Valencia, “Infraestructuras (I) Redes Inalámbricas: Capítulo 11 | Guía de Industria 4.0.” https://ticnegocios.camaravalencia.com/servicios/tendencias/caminar-con-exito-hacia-la-industria-4-0-capitulo-11-infraestructuras-i-redes-inalambricas/ (accessed Apr. 07, 2021).

[25] D. Large and J. Farmer, “Network Architecture - an overview | ScienceDirect Topics,” 2009. https://www.sciencedirect.com/topics/computer-science/network-architecture (accessed Feb. 20, 2021).

[26] R. Salazar-Cabrera and A. Pachon, “Methodology for Design of an Intelligent Transport System (ITS) Architecture for Intermediate Colombian City,” *Ing. Y Compet.*, vol. 21, no. 1, 2019, doi: 10.25100/iyc.v21i1.7654.

[27] M. G. Ruiz Maldonado and E. Inga, “Asignación óptima de recursos de comunicaciones para sistemas de gestión de energía,” *Enfoque UTE*, vol. 10, no. 1, pp. 141–152, 2019, doi: 10.29019/enfoqueute.v10n1.447.

[28] J. Pérez Trigo, *Introducción a los sistemas móviles de comunicaciones*, no. 7. 2019.

[29] M. Zeyad, S. Ghosh, and S. M. Masum Ahmed, “Design prototype of a smart household touch sensitive locker security system based on GSM technology,” *Int. J. Power Electron. Drive Syst.*, vol. 10, no. 4, pp. 1923–1931, 2019, doi: 10.11591/ijpeds.v10.i4.1923-1931.

[30] R. K. Ghosh, “GSM, GPRS and UMTS,” in *Wireless Networking and Mobile Data Management*, Springer, Singapore, 2017, pp. 55–94.

[31] G. A. Chica-pedraza, D. N. Angulo-esguerra, Á. F. Díaz-Sánchez, and M. Espinosa-Buitrago, “Implementación de estación base GSM recepción de señales LTE aplicando radio definido por software,” *Rev. ITECKNE*, vol. 17, no. 1, pp. 19–30, 2020, [Online]. Available: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982020000100019.

[32] A. Parmar, K. M. Pattani, P. G. Student, and C. U. S. College, “Sniffing GSM Traffic Using RTL-SDR And Kali Linux OS,” *Int. Res. J. Eng. Technol.*, vol. 4, no. 1, pp. 1637–1642, 2017, [Online]. Available: https://irjet.net/archives/V4/i1/IRJET-V4I1323.pdf.

[33] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Popper, “On security research towards future mobile network generations,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 2518–2542, 2018, doi: 10.1109/COMST.2018.2820728.

[34] Á. Julieth, M. Delgado, C. Milena, H. Bonilla, V. Manuel, and Q. Flórez, “Algoritmo de control de potencia para el simulador básico a nivel de sistema LTE,” *Entramado*, vol. 14, no. 2, pp. 300–318, 2018.

[35] D. Gutierrez, F. Gimenez, C. Zerbini, and G. Riva, “Measurement of 4G LTE Cells with SDR Technology,” *IEEE Lat. Am. Trans.*, vol. 18, no. 2, pp. 206–213, 2020, doi: 10.1109/TLA.2020.9085272.

[36] J. C. Arantxa Villavicencio, Christian Quispe, Fernando Velásquez, “Evolución hacia la tecnología 5G Requerimientos para 5G,” 2016.

[37] W. S. H. M. W. Ahmad *et al.*, “5G Technology: Towards Dynamic Spectrum Sharing Using Cognitive Radio Networks,” *IEEE Access*, vol. 8, pp. 14460–14488, 2020, doi: 10.1109/ACCESS.2020.2966271.

[38] A. Bahnasse *et al.*, “WiMax technology for maritime intelligent transport systems communication,” *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3231053.3231063.

[39] C. E. Vaca Cano and R. A. Lara Cueva, “Análisis de la calidad de servicio de una red WiMAX en conformidad con el estándar IEEE 802.16-2009 en escenarios exteriores,” *RECI Rev. Iberoam. las Ciencias Comput. e Informática*, vol. 7, no. 13, pp. 43–63, 2018, doi: 10.23913/reci.v7i13.77.

[40] “¿Qué es WiMAX? | eConectia,” *eConectia*, 2019. https://www.econectia.com/blog/que-es-wimax (accessed Apr. 09, 2021).

[41] Ghaliya Alfarsi, “Using Cisco Packet Tracer to simulate Smart Home,” *Int. J. Eng. Res.*, vol. V8, no. 12, 2020, doi: 10.17577/ijertv8is120211.

[42] K. Dejan, “¿Qué es norma ISO 27001?” https://advisera.com/27001academy/es/que-es-iso-27001/ (accessed Apr. 09, 2021).

[43] N. Tuptuk and S. Hailes, “Security of smart manufacturing systems,” *J. Manuf. Syst.*, vol. 47, no. April, pp. 93–106, 2018, doi: 10.1016/j.jmsy.2018.04.007.

[44] Organización Internacional de Normalización ISO, “ISO - 35.030 - Seguridad de TI,” 2015. https://www.iso.org/ics/35.030/x/ (accessed Feb. 20, 2021).

[45] S. A. AGUILAR BRAVO and J. P. APOLO YAGUANA, “IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA ACCESS NET CENTRADO EN LA NORMA ISO/IEC 27001:2013,” Machala, 2020.

[46] Arcotel, “Agencia de Regulación y Control de las Telecomunicaciones – Promovemos el desarrollo armónico del sector de las telecomunicaciones, radio, televisión y las TIC , mediante la administración y regulación

eficiente del espectro radioeléctrico y los servicios." https://www.arcotel.gob.ec/ (accessed Apr. 09, 2021).

[47] SecAware, "ISO/IEC 27033," 2016. https://www.iso27001security.com/html/27033.html.

[48] A. Ochoa, "Diseño de una Red de Seguridad Informatica para la Protección de Sistema Web de un Call Center ante Ataques Informaticos Aplicando la Norma iso 27033," 2019.

[49] J. G. M. Gualda Muñoz, "Estudio de la arquitectura de protocolos de LTE," 2016.

[50] D. I. Chicaiza Cazar, "Modelo de gestión de la seguridad de la información para pequeñas empresas," 2019.

5. ANEXOS

Anexo A: Rutas de buses urbanos

Ilustración 19: Rutas de buses urbanos
Fuente: Elaboración propia

Anexo B: Simulación de red

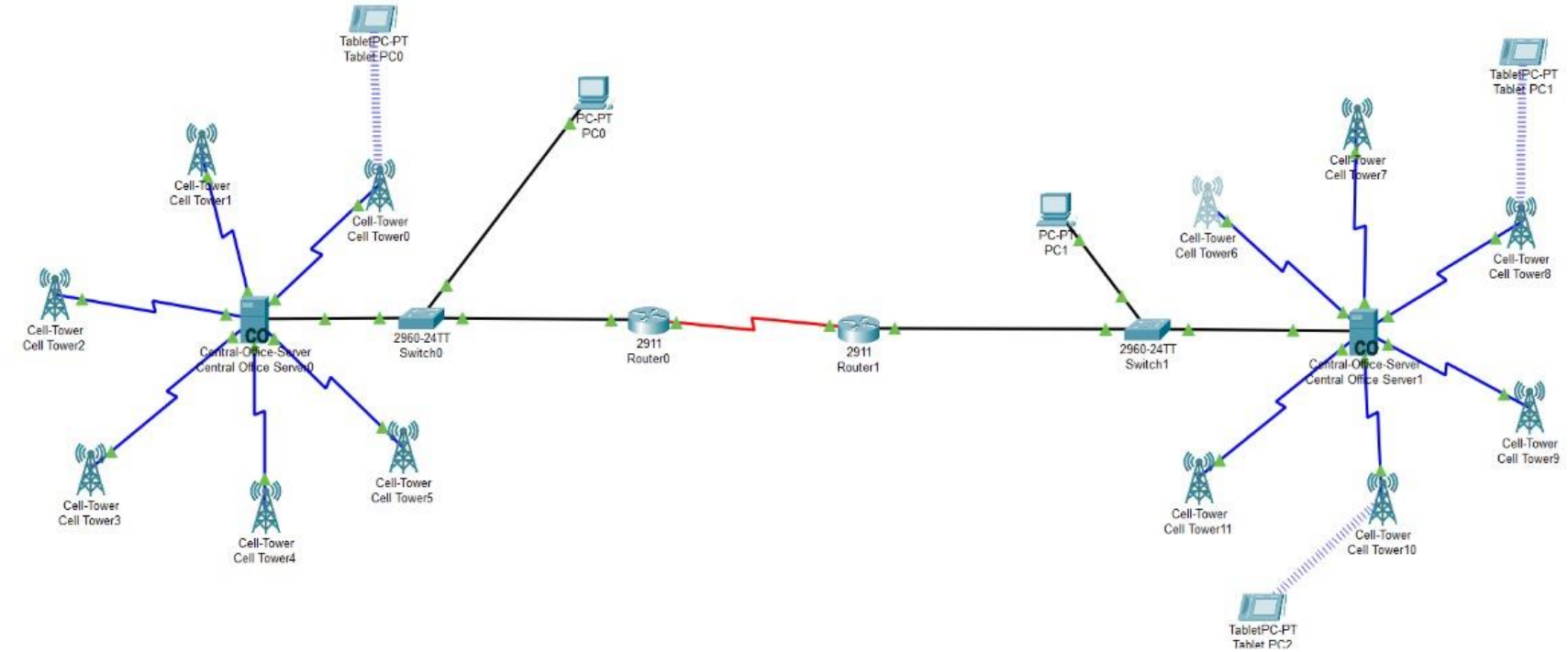


Ilustración 20: Simulación de red
Fuente: Elaboración propia