Diseño de un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del estado a través de dispositivos móvil celular

Jorge Enrique Robles Silva

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

DISEÑO DE UN MODELO DE PLATAFORMA TECNOLÓGICA QUE PERMITA BRINDAR SEGURIDAD A LAS COMUNICACIONES ESTRATÉGICAS DEL ESTADO A TRAVÉS DE DISPOSITIVOS MÓVIL CELULAR.

ALUMNO: JORGE ENRIQUE ROBLES SILVA

DIRECTOR: ING. RAFAEL VICENTE PÁEZ MÉNDEZ

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

Diseño de un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móvil celular.

Elaborado por

Jorge Enrique Robles Silva

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de Grado

Bogotá-Colombia

2019

Ministerio de Defensa Nacional

Comando General de las Fuerzas Militares

Escuela Superior de Guerra

Maestría en Ciberseguridad y Ciberdefensa

Diseño de un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móvil celular.

Elaborado por

Jorge Enrique Robles Silva

Director

Ing. Rafael Vicente Páez Méndez

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de Grado

Bogotá-Colombia

2019

Dedico este trabajo al Todo poderoso porque me guió y me dio toda la fuerza necesaria para poder llegar a este momento tan especial y llenar todos mis caminos con su amor.

Dedico este trabajo a mi hija Catalina, Esposa Ana María, a mis padres Jorge y Amparo y Hermanos John Jairo y Carolina, por que estuvieron presentes en todos esos momentos difíciles y siempre me brindaron su apoyo y amor incondicional.

AGRADECIMIENTOS

Agradezco a Dios por acompañarme en todos mis caminos, en especial en estos momentos tan importantes que curso esta maestría, ya que es un logro más para su gloria y honra de su nombre.

Agradezco a mi esposa Ana María e hija Catalina por tenerme tanta paciencia en este nuevo reto, por su apoyo incondicional que me brindaron en todo momento de alegría y de tropiezos porque siempre estuvieron ahí para brindarme su apoyo.

A mis padres Jorge y Amparo por apoyarme en todo momento, por sus valores inculcados y por el esfuerzo realizado de haberme dado una buena educación en todas sus formas durante todo mi camino en esta vida. Y gracias por ser mi ejemplo de vida a seguir.

A mi empresa, por darme la oportunidad de fortalecerme profesionalmente y brindarme todo el apoyo necesario para poder llegar hasta aquí con éxitos ya que es una de las muchas metas trazadas en mi vida.

Agradezco a mi director de tesis el Doctor Rafael Vicente Páez Méndez, que con su conocimiento y experiencia me orientó y encaminó en todo momento para llegar a este punto que significa mucho para mí.

Resumen Ejecutivo

El objetivo del presente trabajo de investigación corresponde a la necesidad actual de homologar un modelo de seguridad en las comunicaciones móviles, que puedan ser utilizados en las instalaciones públicas del Estado, a fin de evitar la consumación de riesgos relacionados con la interceptación ilegal de comunicaciones, fuga de información y revelación de información con reserva legal, teniendo en cuenta las interceptaciones ilegales presentadas anteriormente en el Estado Colombiano en los últimos 5 años como ha sido el caso conocido "Andrómeda el 23 de enero de 2014" que según (Palma, 2018) del diario El Espectador "hacían transacciones con información clasificada e interceptaban comunicaciones privadas relacionadas con el proceso de paz", el otro caso sonado en el 2018 el del "General(r) Humberto Guatibonza" según (Redacción Judicial El Espectador, 2019) "donde el General(r) ofrecía los servicios de interceptación telefónica y de WhatsApp" entre otras.

Por lo anterior y teniendo en cuenta a los antecedentes mencionados, toda la información que se transmite a través de los medios de telefonía móvil es susceptibles a interceptaciones ilegales, por tal motivo es de importancia realizar un modelo que permita realizar comunicaciones móviles de forma segura entre funcionarios del alto gobierno mitigando así la fuga de información que por este medio se transmite.

Para el desarrollo de esta investigación se ha propuesto una metodología analítica-descriptiva, que permita encontrar un modelo que se adapte a las necesidades que se expondrán en el transcurso de esta investigación.

En el **capítulo uno** se introduce a la teoría relacionado con la telefonía móvil celular y su evolución; en el **capítulo dos**, se describe las vulnerabilidades más conocidas que se presentan en

las diferentes tecnologías de comunicación como lo son GSM, GPRS, UMTS, LTE; en el **capítulo tres**, se expondrán algunas soluciones de seguridad que permitan minimizar las amenazas que asechan el uso seguro de la telefonía móvil y en el **capítulo cuatro**, se describe el modelo que se empleará para el desarrollo de la plataforma móvil celular el cual permitirá asegurar las comunicaciones estratégicas que se realicen a través de la telefonía móvil.

Si bien, hay modelos de comunicaciones móviles seguras que ya existen en el mercado, estos no proporcionan una confidencialidad en las comunicaciones.

Palabras claves: Vulnerabilidades, riesgos, cifrado extremo a extremo, dispositivo móvil, modelo, algoritmos.

Abstract

The objective of this research work corresponds to the current need to homologate a security model in mobile communications, which can be used in public facilities of the State, in order to avoid the consummation of risks related to the illegal interception of communications, leakage of information and disclosure of information with legal reserve, taking into account the illegal interceptions previously presented in the Colombian State in the last 5 years, such as the case known as "Andromeda on January 23, 2014," which according to (PALMA, 2018) of the newspaper El Espectador "made transactions with classified information and intercepted private communications related to the peace process, the other case sounded in 2018 was the "General(r) Humberto Guatibonza" according to (Redacción Judicial El Espectador, 2019) "where the General(r) offered the services of telephone interception and WhatsApp" among others.

For this reason, it is important to develop a model that allows to secure mobile communications between important heads of high government, thus mitigating the leakage of information that is transmitted through this medium.

For the development of this research, an analytical-descriptive methodology has been proposed, which allows to find a model that adapts to the needs that will be exposed in the course of this research.

Chapter one introduces the theory related to mobile cellular telephony and its evolution; chapter two describes the best-known vulnerabilities in different communication technologies such as GSM, GPRS, UMTS, LTE; chapter three describes some security solutions to minimize threats to secure use of mobile telephony; and chapter four describes the model to be used for the development of the mobile cellular platform, which will ensure strategic communications through mobile telephony.

Although there are models of secure mobile communications that already exist in the market, they do not provide confidentiality in communications as they do not meet the requirements that are being exposed in this research because they do not comply with the security measures that will be exposed in this research.

Keywords: Vulnerabilities, risks, end-to-end encryption, mobile device, model, algorithm

Lista de abreviaturas y siglas

RTC	:	Redes de Telefonía conmutada
RDSI	:	Red Digital de Servicios Integrados
ADSL	:	Línea de Suscriptor Digital Asimétrico.
LAN	:	Red de Área Local.
CNABF	:	Cuadro Nacional de Atribuciones de Banda de Frecuencia.
TMA	:	Telefonía Móvil Automática.
TM	:	Telefonía Móvil.
STB	:	Servicio Telefónico Básico.
AMPS	:	Sistema Telefónico Móvil Avanzado.
FM	:	Frecuencia Modulada.
FSK	:	Modulación por Desplazamiento de Frecuencia
GSM	:	Comunicaciones Móviles para Sistemas Globales.
TDMA	:	Acceso Múltiple por División de Tiempo.
PCS	:	Servicio de Comunicación Personal.
GPRS	:	General Packet Radio Service.
UMTS	:	Sistema de Telecomunicaciones Móviles Universales.
LTE	:	Evolución a Largo Plazo.
WCDMA	:	Acceso Múltiple por División de Código de Banda Ancha.
HSDPA	:	Acceso Descendentes de Paquetes a Alta Velocidad.
HSUPA	:	Acceso Ascendentes de Paquetes a Alta Velocidad.
HSPA	:	Acceso de Paquetes a Alta Velocidad.

IP	:	Protocolos de Internet.
MITM	:	Hombre en el medio.
MS	:	Estación Móvil.
BSS	:	Subsistema de Estación Base.
NSS	:	Subsistema de Conmutación de Red.
BTS	:	Estación Base Transceptora.
BSC	:	Controlador de Estaciones Base.
MSC	:	Centro de Comunicación Móvil.
MS	:	Estación Móvil.
ME	:	Dispositivo Móvil.
EMCP	:	Protocolo de cifrado de contenido móvil.
TMSI	:	Identidad del subscriptor móvil temporal.
IMSI	:	Identidad Internacional del Abonado Móvil.
E-UTRAN	:	Redes de acceso de radio terrestre evolucionada.
UE	:	Equipo móviles de usuarios.
EPC	:	Red troncal de paquetes evolucionada
MME	:	Área de gestión de la movilidad

Tabla de Contenido

Tabla de Imágenes

Lista de Tablas

Introducción

El uso de teléfonos móviles a nivel mundial ha ido en crecimiento según la firma RBC Capital Market, que de 7.450 millones de personas en el mundo el 75% de la población mundial usa un teléfono móvil (Díaz, 2011).

Por tal motivo, el aumento de esta tecnología ha convertido a las personas a depender de este medio, se vive en una sociedad consumista de información y se comparte gran parte de la vida en línea. Se vive en un mundo en el que la demanda de acceso a la información en plataformas móviles crece a un ritmo acelerado, las personas quieren estar viendo el correo electrónico, ver perfil de amigos en Facebook, saber dónde está el café más cercano y estar al tanto de lo que ocurre en el mundo, desde su teléfono móvil.

Los dispositivos móviles celular han evolucionado de una manera acelerada, hace 20 años un teléfono móvil solo se usaba para hablar y enviar mensajes de texto, el acceso a los datos móviles se consideraba limitados y muy costosos, y no todas las personas podían tener acceso a la web, el uso de los computadores era mayor y existía más demanda de esta tecnología.

Actualmente, un *Smartphone* como son llamados hoy día ha revolucionado el mundo tecnológico convirtiendo estos dispositivos en un medio imprescindible para las personas, el manejo de los datos es alcanzable para todas las comunidades ya que en varias áreas de las ciudades se puede encontrar sitios que poseen una red wifi gratis. Los dispositivos poseen tecnología equivalente a los de un computador haciendo que estos permitan realizar actividades similares por donde pasa todo tipo de información personal, de la empresa, bancaria etc., y lo mejor de todo que se pueden portar en el bolsillo.

Según José Ignacio Niño González en su publicación "La importancia del teléfono móvil para la comunicación publicitaria" expresa que la revolución móvil, ha roto los estándares vigentes

y ha propiciado un nuevo modo de interrelación basado en la movilidad que permite al ser humano estar conectado en cualquier lugar, (González, 2013).

La inseguridad que se presenta en las comunicaciones que se realizan a través de los dispositivos móviles son cada vez más comunes, por ejemplo, el incremento de interceptaciones ilegales mediante el empleo de estaciones bases transceptoras (por sus siglas en inglés, Base Transceiver Station, en adelante BTS) falsas, la captura de tráfico GSM, los ataques de hombre en el medio (por sus siglas en inglés, Man In The Middle, en adelante MITM), y la suplantación de usuarios son algunos de las debilidades que se presentan en las comunicaciones de telefonía móvil y esto es, en parte, causado por la débil infraestructura tecnológica que poseen los operadores de telefonía móvil.

Las comunicaciones móviles son vulnerables, porque han sido objeto de control de Estados, organizaciones criminales, delincuencia organizada, utilizando capacidades que se pueden adquirir en la web a bajo costo, conllevando así al aumento del riesgo en pérdida de la confidencialidad, integridad y disponibilidad de las comunicaciones, acrecentando así la perdida de la privacidad de la información en las comunicaciones entre las personas.

Por tal motivo es importante tener en cuenta que las comunicaciones que se realizan a nivel de Estado a través de los dispositivos de telefonía móvil celular deben tener un tratamiento especial en el manejo de la información que se transmite por estos medios. Debido a lo anterior surge la siguiente pregunta de investigación: ¿cuál podría ser el modelo de plataforma tecnológica que genere condiciones de seguridad a las comunicaciones estratégicas del Estado en los dispositivos móviles celular?

1. Objetivo del proyecto

1.1. Objetivo General

Diseñar un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móviles celulares.

1.2. Específicos

- Identificar las vulnerabilidades presentes en las comunicaciones de telefonía móvil Celular.
- Explicar cómo contrarrestar el riesgo asociado a las vulnerabilidades presentes en las comunicaciones móviles celulares.
- Desarrollar una propuesta de modelo tecnológico que permita asegurar las comunicaciones estratégicas del Estado.

1.3. Metodología

El diseño metodológico por el cual se basa esta investigación será mediante el método deductivo indirecto ya que se desarrollará de lo general a lo particular. Evidenciando una investigación general de las diferentes arquitecturas de comunicación móviles seguras, aterrizando esta idea en un modelo topológico específico que se ajuste a la necesidad de las comunicaciones estratégicas del Estado, como se muestra en la Imagen 1.

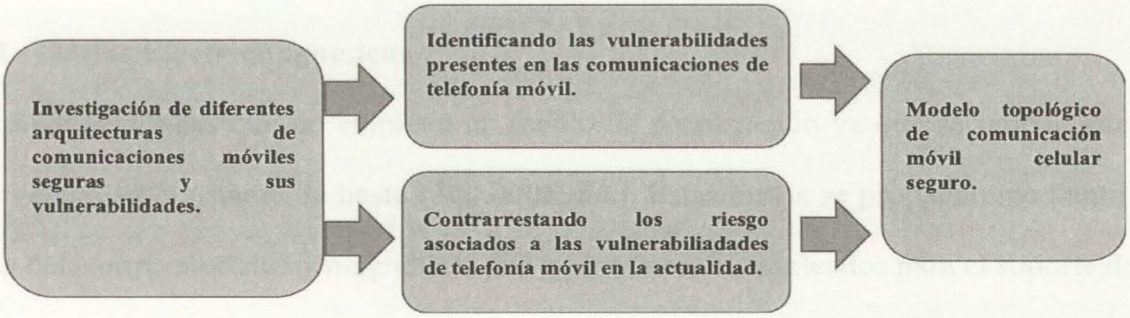


Imagen 1. Diagrama de bloques del modelo topológico de comunicación móvil celular segura

Por lo anterior, se desarrollará un diseño metodológico que permitirá conseguir el modelo propuesto, y para llevarlo a cabo, se identificarán las vulnerabilidades actuales presentes en la comunicación móvil y se expondrán las diferentes formas de contrarrestar dichas vulnerabilidades, para así, poder desarrollar un modelo topológico que permitirá brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móviles celulares.

2. Marco Teórico

Para el diseño de un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones de dispositivos móviles celulares en las comunicaciones estratégicas del Estado, es importante conocer como es el funcionamiento de la comunicación móvil celular, su evolución, sus vulnerabilidades y el por qué las comunicaciones son inseguras. A través de este documento se podrá profundizar en la historia de las telecomunicaciones, el teléfono, el espectro radioeléctrico, la comunicación de los teléfonos fijos, la telefonía móvil, los sistemas celulares, la seguridad en las comunicaciones y que son las interceptaciones ilegales en las comunicaciones dando así una descripción del problema que se quiere tratar y el porqué de la importancia de desarrollar un modelo para asegurar las comunicaciones que se realizan en las entidades del Estado.

2.1.Historia de las Telecomunicaciones

2.1.1. Ondas Electromagnéticas

Son aquellas Ondas que no emplean un medio de propagación ya que se propagan en el vacío a una velocidad constante de hasta (300.000Km/s). Estas ondas se propagan mediante una estimulación del campo eléctrico y magnético, por tal motivo son empleados para el soporte de las telecomunicaciones y el funcionamiento complejo del mundo actual. (John R. Pierce, 2002)

2.1.2. Frecuencia

La frecuencia es la cantidad de veces que se repite un movimiento periódico, cada inversión completa de una onda se llama ciclo, su unidad básica es el Hertz (Hz), y se contabiliza como un Hertz, que es igual a un ciclo por segundo. (1Hz=1cps). (Tomasi, 2003).

2.1.3. El Espectro Radioeléctrico

El espectro radio eléctrico es el medio por el cual se transmiten las frecuencias de ondas de radio electromagnéticas que permiten el funcionamiento de las telecomunicaciones de radio, internet, telefonía móvil, televisión digital terrestre, entre otras, y son administradas y reguladas por el gobierno de cada país.

Según la constitución política de Colombia dice: "El espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado".

La asignación de una banda de frecuencia se realiza mediante una autorización, la cual permite hacer uso específico de la misma con unas condiciones determinadas. (Judicatura, 1991).

Así mismo el espectro radioeléctrico está dividido en bandas de frecuencias, las cuales le otorgan una porción a cada servicio de telecomunicaciones así:

VLF: Frecuencia muy baja, comprende las bandas de 3 KHz a 30 KHz.

LF: Frecuencia baja, comprendida entre las bandas 30 KHz a 300 KHz.

MF: Frecuencia media, que comprende las frecuencias entre 300 KHz a 3000 KHz.

HF: Alta frecuencia, que comprende las frecuencias entre 3 MHz a 30 MHz.

VHF: Muy alta frecuencia, se encuentra en los rangos entre 30 MHz a 300 MHZ

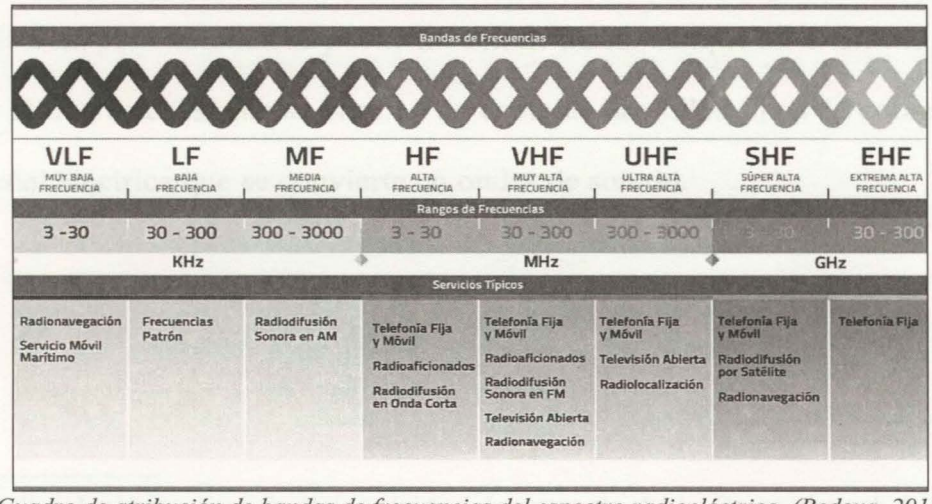
UHF: Ultra alta frecuencia, maneja rangos entre 300 MHz a 3000 MHz

SHF: Súper alta frecuencia, maneja rangos entre 3 GHz a 30 GHz

Por tal motivo toda la información que por este medio se transmite está quedando expuesta a personas mal intencionadas que pueden interceptarlas mediante la implementación de equipos diseñados para estos fines. (Espectro, 2017).

2.1.4. Cuadro Nacional de Atribuciones de Frecuencias

El cuadro nacional de atribuciones de banda de frecuencia (CNABF) por sus siglas, es un instrumento que se usa en la gestión, administración y control del espacio radioeléctrico, en este cuadro se encuentran consignados, entre otros, la normatividad asociada con la atribución del espectro radioeléctrico en Colombia a los servicios de radiocomunicaciones y los planes de distribución de canales de estos. Como se aprecia en la Imagen 2.



Imágen 2. Cuadro de atribución de bandas de frecuencias del espectro radioeléctrico. (Bedoya, 2012)

2.1.5. El Teléfono

El teléfono es un dispositivo de telecomunicación diseñado para transmitir conversaciones por medio de señales eléctricas. Su creador en principio se le atribuyó al científico a Alexander Graham Bell[1] en 1876 pero solo hasta el 2002 el congreso de Estados Unidos aprobó la resolución 269 donde afirmaba que el verdadero inventor del teléfono fue Antonio Meucci[2] y no Graham Bell. (Joskowicz, 2015)

El teléfono básicamente se constituía en un emisor y un receptor que se comunicaban mediante un cable de conexión, el sistema estaba conformado por un diafragma metálico flexible y un embobinado, el modo de operar este dispositivo era a través de las ondas de sonido que se emitían chocando sobre el diafragma haciendo vibrar el campo magnético del imán de la bobina, produciendo una corriente en la bobina que cambiaba según las vibraciones del diafragma.

2.1.6. Teléfonos Fijos

Al pasar el tiempo la forma de comunicarse ha evolucionado y con ella su tecnología, en la actualidad se habla de 3 formas de comunicaciones fijas: análoga, digital, IP.

Líneas analógicas consiste en redes de telefonía conmutada conocida como (RTC), pensada en transmisión de la voz, pero también se puede transmitir datos, aunque no al mismo tiempo. Un ejemplo de esto es el fax, este sistema se basa en un cable de dos hilos finos de cobre por el cual se transmite una señal eléctrica que se convierte en ondas de sonido.

---

[1] Alexander Graham Bell (Edimburgo, Escocia, Reino Unido 3 de marzo de 1847 – Beinn Bhreagh, isla del cabo Bretón, Canadá 2 de agosto de 1922) científico, inventor y logopeda británico.

[2] Antonio Meucci (Florencia, Italia 13 de abril de 1808 – New York, 18 de octubre de 1889) inventor italiano, creador del teléfono; posteriormente bautizado como "teléfono", entre otras innovaciones técnicas.

2.2.Telefonía Móvil Celular

Los sistemas de comunicaciones son elementos que permiten la transmisión de sonidos a larga distancia mediante medios eléctricos o electromagnéticos, los cuales permiten realizar y recibir llamadas desde cualquier lugar siempre que esté dentro del área de cobertura del servicio que lo facilita.

Una red o servicio de este tipo, cuyos usuarios son individuales, es lo que se denominó inicialmente Telefonía Móvil Automática o TMA, utilizándose ahora, simplemente, el termino TM o celular.

Según Hidobro. J y Conesa. R. (2006) dice: "que el servicio de la telefonía móvil está concebido como una extensión del servicio telefónico básico (STB), posibilitando el establecimiento de comunicaciones desde aparatos terminales de abonado que no tienen por qué estar asociados a un lugar determinado".

Actualmente, en el mundo, existen dos modalidades, que son de transmisión analógica y transmisión digital, siendo la analógica de aparición anterior a la digital.

Según el autor Francisco Barceló y Javier Jordán "En los últimos años hemos asistido a la implantación y desarrollo de las redes de comunicaciones móviles por parte de los operadores, y al rápido crecimiento de este mercado, que tiene escasos precedentes en el mundo de la tecnología". (Francisco Barceló, 2002). A lo largo de este proceso, no ha sido siempre fácil conjugar la necesaria rapidez de implantación con una planificación mesurada y acorde a las necesidades reales de los usuarios. Una planificación con escasos recursos deja al operador prestando servicios de baja calidad, y problemas de seguridad para los usuarios que es al final el afectado por la mala planeación de las infraestructuras tecnológicas.

El crecimiento de la demanda de los servicios de telefonía móvil analógica en los años 80 y principios de los 90, planteó problemas en la capacidad de los sistemas saturando literalmente el espectro radioeléctrico hecho que estimuló el desarrollo de los sistemas digitales, con mayor soporte en cuanto a número de usuarios y una mayor calidad, siendo estos últimos los que predominan en la actualidad y estando los otros en vía de desaparición.

Estos sistemas se denominan celulares porque se sustentan en dos conceptos principales, que son: la reutilización de frecuencias y dimensionamiento celular por medio de hexágonos regulares, a modo de una colmena de abejas, como se ilustra en la Imagen 3. (Jose Manuel Huidobro Moya, 2006)

La telefonía móvil ha evolucionado en el transcurso del tiempo y los servicios que cubre la telefonía inalámbrica, están destinados a suministrar el acceso a las redes fijas públicas a personas en movimiento y se pueden distinguir los siguientes tipos de servicios:

- Centro de conmutación móvil (del inglés *Mobile Switching Center*, en adelante MSC): es el sistema que permite conectar las llamadas entre usuarios móviles.
- La red telefónica pública conmutada (del inglés *Public Switching Telephone Network*, en adelante PSTN): es un sistema de circuitos que permite conmutar las comunicaciones de vos en tiempo real.
- Controladores de estación base (de sus siglas en inglés *Base Station Controller*, en adelante BSC): maneja los recursos de radio de las BTSs y maneja las frecuencias usadas, los saltos en frecuencia y el paso entre las celdas de las estaciones móviles (del inglés *Mobile Station,* en adelante MS).

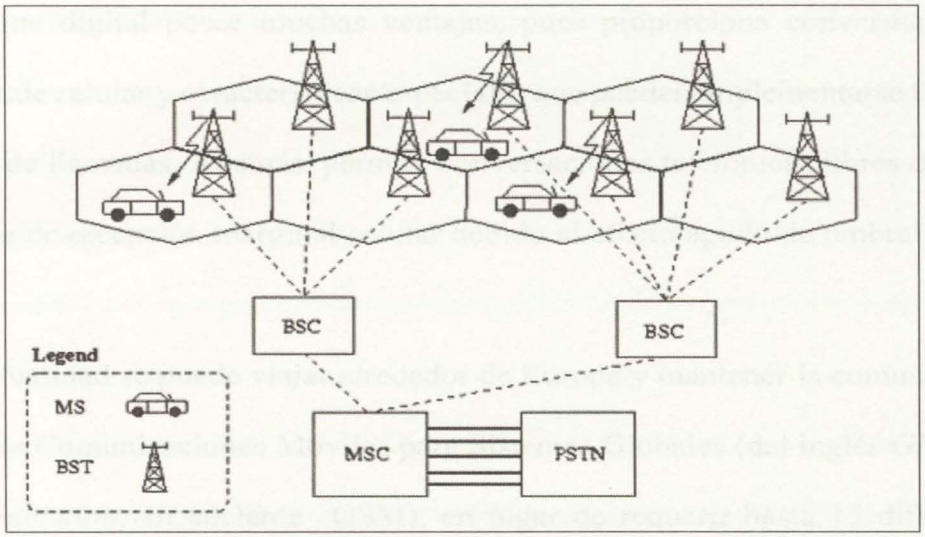


Imagen 3. Sistema Básico de Telefonía Celular. (Alison, 2011)

2.2.1. Primera generación (1G), el sistema análogo.

Los sistemas de telefonía celular de primera generación (1G) empleado en Estados Unidos fue el sistema telefónico móvil avanzado (*Advanced Mobile Phone System* - AMPS), el cuál fue desarrollado por AT&T[3] y Motorola[4].

Éste es un sistema analógico, ya que usa la señal de audio de frecuencias de voz (por sus siglas en inglés, *voice frequency* en adelante VF) para modular por frecuencia (FM) a una portadora. Para implementar este concepto de AMPS en Estados Unidos, se debió encontrar espacio espectral para su asignación. Esto se logró con la banda de 806 a 890 MHz.

2.2.2. Segunda generación (2G), el sistema digital

La señal analógica se convierte a un flujo digital de bits comprimidos, el cual es modulado sobre una portadora. La velocidad de bit de los datos comprimidos se diseña para que sea relativamente pequeña, de tal forma que se pueda soportar un gran número de usuarios.

[3] AT&T: Compañía Estadounidense de telecomunicaciones
[4] Motorola: Empresa estadounidense especializada en la electrónica y la stelecomunicaciones, establecida en Schaumburg, Illinois, a las afueras de Chicago.

El enfoque digital posee muchas ventajas, pues proporciona conversaciones privadas, resistencia a fraude celular y características especiales que pueden implementarse fácilmente como el identificador de llamadas. Además, permite conversaciones telefónicas libres de ruido hasta el límite de la zona de recepción marginal celular debido al efecto agudo de umbral de los sistemas digitales.

En la actualidad se puede viajar alrededor de Europa y mantener la comunicación a través de un teléfono de Comunicaciones Móviles para Sistemas Globales (del inglés *Global System for Mobile Communication*, en adelante GSM), en lugar de requerir hasta 15 diferentes tipos de teléfonos celulares de 1G. GSM utiliza acceso múltiple por división de tiempo (del inglés *Time Division Múltiple Access*, en adelante TDMA), que proporciona ranuras de tiempo para soportar hasta ocho usuarios en cada canal de 200 kHz de ancho. El teléfono GSM se programa para una cuenta de usuario en particular mediante una tarjeta inteligente incorporada, la cual contiene el número telefónico del usuario y otra información de cuenta. (Jose Manuel Huidobro Moya, 2006)

Para proporcionar más competición celular en Estados Unidos, la Comisión de Comunicaciones Federales (de sus siglas en inglés, *Federal Communication Commission*, en adelante FCC), ha reasignado las frecuencias en la banda de 1.9 GHz del servicio por microondas de punto a punto al Servicio de Comunicación Personal (de sus siglas en inglés, *Personal Communication Service*, en adelante PCS), celular. Las bandas asignadas para la comunicación 2G es de 1,850 MHz a 1,990 MHz. (Jose Manuel Huidobro Moya, 2006).

2.2.3. Tercera generación (3G)

El estándar de la tercera generación 3G permitirá a los usuarios inalámbricos hacer *roaming* mundialmente con un solo teléfono así mismo permite la transmisión de voz y datos a través de la telefonía móvil mediante el sistema de telecomunicaciones móviles universales (del inglés

Universal Mobile Telecommunication System, en adelante, UMTS). Los servicios asociados a la tercera generación permiten la descarga de programas, intercambio de correos electrónicos y mensajería instantánea.

La mayoría de los móviles 3G soportan su uso como módem USB (soportado por todos los teléfonos inteligentes con sistemas operativos Android[5] y iOS[6] y algunos permiten su uso vía Wi-Fi y Bluetooth.

Las redes 3G ofrecen mayor grado de seguridad en comparación con sus predecesoras 2G, al permitir al equipo del usuario (del inglés *User Equipment*, en adelante UE) autenticar la red a la que se está conectando. (Jose Manuel Huidobro Moya, 2006).

2.2.4. Cuarta generación (4G)

Las comunicaciones móviles de cuarta generación están caracterizadas por contar con dos tecnologías alternativas o complementarias, según la situación particular de cada operador móvil. Ambas comparten muchas similitudes e incluso podrían llegar a converger.

Las dos tecnologías que más adeptos tienen son: Evolución a Largo Plazo Avanzado (de sus siglas en inglés, *Long Term Evolution Advance,* en adelante LTE) y Wireless MAN-Advanced. El eje de trabajo que acá se reporta lo constituyen el análisis del desarrollo que estas dos tecnologías tienen actualmente y su contribución a la implementación de soluciones 4G. (Jose Manuel Huidobro Moya, 2006).

La tecnología LTE, es considerado por muchos como el sucesor obvio para la actual generación de la tecnología 3G UMTS, que está basado en WCDMA, HSDPA, HSUPA y HSPA. LTE no es un sustituto de UMTS en la manera en que UMTS fue un reemplazo para el GSM, sino

[5] Android: Sistema operativo basado en el núcleo Linux.
[6] IOS: Iphone Operating System, sistema operativo de la empresa Apple Inc.

más bien una actualización de la tecnología UMTS que le permitirá ofrecer velocidades de datos mucho más rápido tanto para la carga y descarga.

Para los consumidores, "LTE permitirá a las aplicaciones existentes poder correr más rápido, además de poner a disposición de las nuevas aplicaciones de telefonía móvil como son: aplicaciones de video mejorado y la presentación del teléfono móvil puede ser incluido". (Jose Manuel Huidobro Moya, 2006)

Por tal motivo como se puede apreciar, actualmente entre más avanzan las tecnologías de telecomunicaciones sin importar el sistema que tengamos de 1ª, 2ª, 3ª o 4ª generación, la información que se transfiere siempre es y será vulnerable.

2.3. Seguridad en las Comunicaciones

Para poder tener una visión más clara del por qué las comunicaciones móviles celulares son inseguras se hace necesario conocer el funcionamiento de un sistema móvil celular.

Para establecer una comunicación móvil celular se debe hacer una división de un área geográfica, por ejemplo, una ciudad, dividiéndola en pequeñas células o celdas para la reutilización de frecuencias a través de la ciudad, permitiendo que varias personas utilicen sus teléfonos al mismo tiempo. Dado lo anterior, cada celda cuenta con su transmisor cuyo fin es la de hacer las veces de estación base, y así poder dar una mayor cobertura en diferentes espacios, para proveer cobertura de radio sobre un área más grande.

Dentro de las características importantes que tiene un sistema celular es las de manejar gran capacidad de usuarios, utilización eficiente del espectro, tener una amplia cobertura.

Un tema importante es que el enlace entre terminal y la red debe mantenerse, cuando ésta pasa de una célula a otra, esta definición es conocida como *Handover*[7].

En la Imagen 4; se presenta una estructura básica de una red de telefonía móvil celular cuya función es la de permitir la comunicación entre dos usuarios, de la siguiente manera:

La estructura se divide en tres (3) grandes áreas: Estaciones Móviles (en adelante MS), Subsistemas de Estaciones Base (en adelante BSS) y los Subsistemas de Conmutación de Red (en adelante NSS).

El Dispositivo Móvil (del inglés, *Mobile Equipment*, en adelante ME) el cual posee una SIM Card, que permite la autenticación con la empresa operadora del servicio de telefonía móvil. Una vez el usuario realiza una llamada esta señal se propaga por el aire conectándose a una celda o a una zona delimitada en forma pentagonal donde se encuentra una BTS, que comprende los dispositivos de transmisión y recepción de radio, cada BTS presta el servicio a una única celda. Posteriormente la señal recibida por la BTS se transmite hacia la BSC, cuya función es la de gestionar los recursos de radio de una BTS. Seguidamente el controlador de la estación base (BSC) se comunica con el Centro de Conmutación Móvil (MSC), siendo éste el componente central del subsistema conmutado de la red (del inglés *Network and Switching Subsystem*, en adelante NSS), quien actúa coordinando y conectando las llamadas entre usuarios móviles. (Jose Pico García, 2014)

[7] Handover: sistema utilizado en comunicaciones móviles celulares con el objetivo de transferir el servicio de una estación base a otra cuando la calidad del enlace es insuficiente en una de las estaciones.

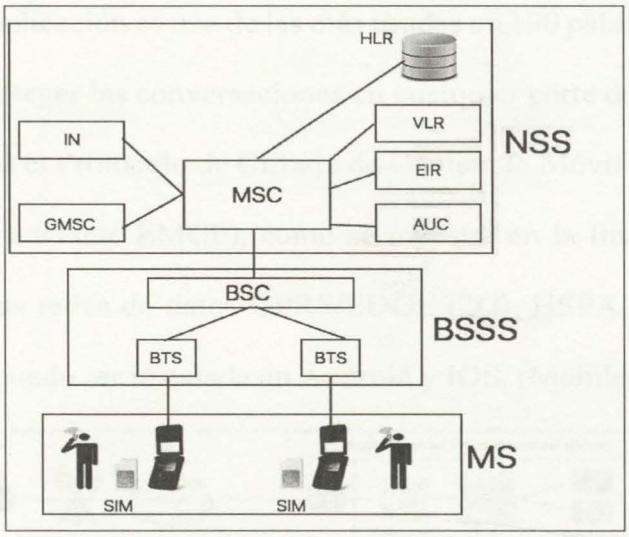


Imagen 4. Estructura de una red de telefonía móvil. Elaboración propia.

2.4. Análisis de Herramientas Existentes

En la actualidad los dispositivos móviles nuevos (*SmartPhones*) están implementando mecanismos de seguridad cada vez más sofisticados tanto en hardware como en software; como son los sensores de huella dactilares, escáneres de iris, cifrado, entre otros controles de seguridad.

Sin embargo, a pesar de la seguridad que puede tener el móvil, las llamadas y los mensajes de texto siguen siendo vulnerables a ataques, ya que existen vulnerabilidades críticas inherentes a los teléfonos móviles y las redes móviles que ponen en riesgo la privacidad de la información personal y la confidencialidad de las organizaciones.

Por lo anterior, existen herramientas de software y hardware en el mercado, que permiten mitigar esas vulnerabilidades inherentes, en la tabla 1 se puede apreciar las ventajas y desventajas que tienen las siguientes herramientas mas comunes empleadas para asegurar las comunicaciones.

2.4.1. Cellcrypt

Cellcrypt es una aplicación desarrollada por Mobile High Security (Reino Unido), que permite realizar comunicaciones cifradas entre usuarios que posean la aplicación mediante

tecnología voz sobre IP, esta aplicación es una de las más usadas en 190 países, su forma de empleo es de pago, el cual permite proteger las conversaciones en cualquier parte del mundo, el protocolo empleado en esta aplicación es el Protocolo de Cifrado de Contenido Móvil (del, inglés *Encrypted Mobile Content Protocol*, en adelante EMCP), como se muestra en la Imagen 5. La tecnología Cellcrypt opera a través de las redes de datos GPRS/EDGE (2G), HSPA, CDMA (3G), WIF y SATELITE, y su plataforma puede ser instalada en Android y IOS. (Mobile High Security, 2012).

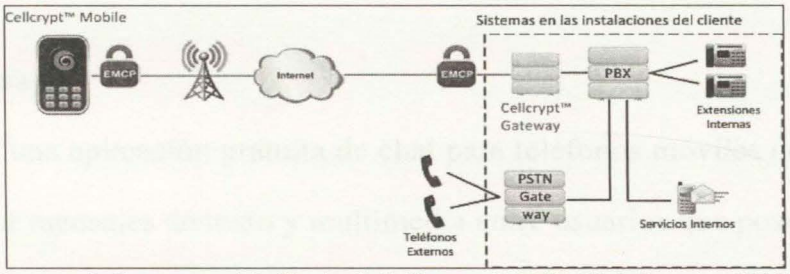


Imagen 5. Estructura del cifrado de Cellcrypt. (Mobile High Security, 2012)

2.4.2. Cryptophone

Cryptophone es una herramienta desarrollada por la empresa GSMK (Alemania), que consiste en un teléfono móvil que brinda seguridad contra escuchas ilegales y vigilancia electrónica mediante el uso de algoritmos que cifran las señales, estos dispositivos poseen un chip criptográfico que permite manejar el cifrado y descifrado de las comunicaciones. En la Imagen 6 se aprecia la estructura del cifrado Twofish de la herramienta del Cryptophone. El chip tiene internamente dos (2) algoritmos que están programados de la siguiente manera: el primer algoritmo encargado del intercambio de claves y el segundo tiene un algoritmo de clave simétrica para el cifrado de la voz.

La herramienta opera en redes 2G, 3G, WIFI, y su plataforma es Windows phone y Android. (Simonite, 2014).

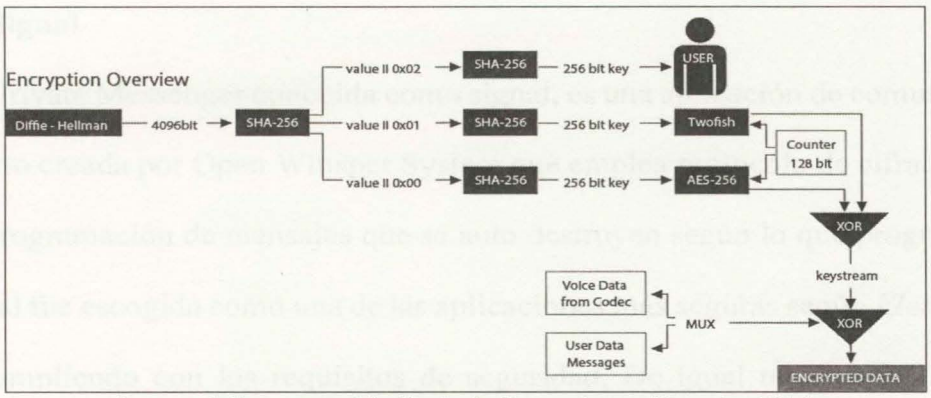


Imagen 6. Estructura del cifrado de Cryptophone. (Simonite, 2014)

2.4.3. Whatsapp

Whatsapp es una aplicación gratuita de chat para teléfonos móviles de última generación, empleado para enviar mensajes de texto y multimedia entre usuarios que posean la aplicación.

Whatsapp tiene un sistema de cifrado de extremo a extremo basada en el protocolo signal diseñado por Open Whisper System como se muestra en la Imagen 7, que funciona mediante el almacenamiento de esas claves del cifrado en el dispositivo de cada usuario.

El sistema hace uso de tres (3) tipos de llave pública, la primera que permite identificar el dispositivo, la segunda es una llave que se genera periódicamente y firmada digitalmente por la anterior, y la tercera que se usa solo una vez en cada utilización del servicio. (METZ, 2016), la aplicación de Whatsapp se emplea en plataformas Android y IOS.

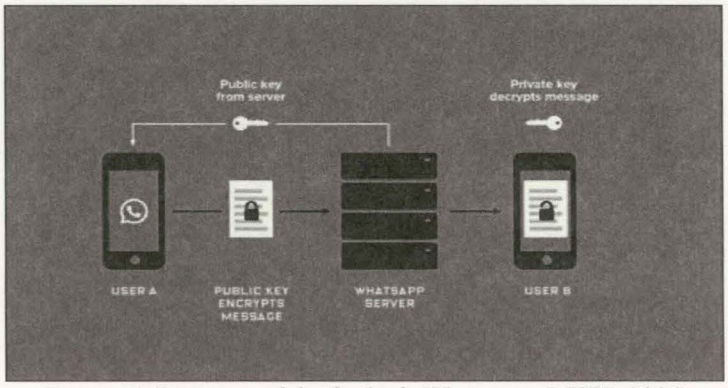


Imagen 7. Estructura del cifrado de Whatsapp. (METZ, 2016)

2.4.4. Signal

Signal Private Messenger conocida como signal, es una aplicación de comunicación segura de código abierto creada por Open Whisper System que emplea protocolo de cifrado de extremo a extremo, con programación de mensajes que se auto destruyen según lo que programe el usuario, en el 2018 signal fue escogida como una de las aplicaciones más seguras según *Electrónic Frontier Foundation*, cumpliendo con los requisitos de seguridad. De igual manera esta aplicación fue recomendad por Edwar Snowden ("exintegrante de la comunidad de inteligencia de los Estados Unidos, quien reveló una serie de programas secretos de vigilancia que emplea la NSA"). (Diario Información, 2018), La plataforma que emplea esta aplicación es IOS y Android.

2.4.5. Telegram

Telegram es una aplicación de mensajería y de llamada segura de VoIP con cifrado de extremo a extremo con sincronización constante en la nube, Telegram fue desarrollada en el 2013, está enfocada en la mensajería instantánea y envío de archivos multimedia en general (tales como Doc, Zip, Mp3 etc..). La infraestructura de Telegram emplea tecnología MTProto cuyo código está abierto empleando cifrado AES 256 a base de API Java como se puede ver en la Imagen 8.

Para los chats normales, Telegram emplea cifrado cliente – servidor – cliente, por otro lado, los receptores llevan una clave compartida firmada en Sha256 para garantizar la integridad de estos. (247 Tecno, 2017). La plataforma que emplea esta aplicación es IOS, Android.

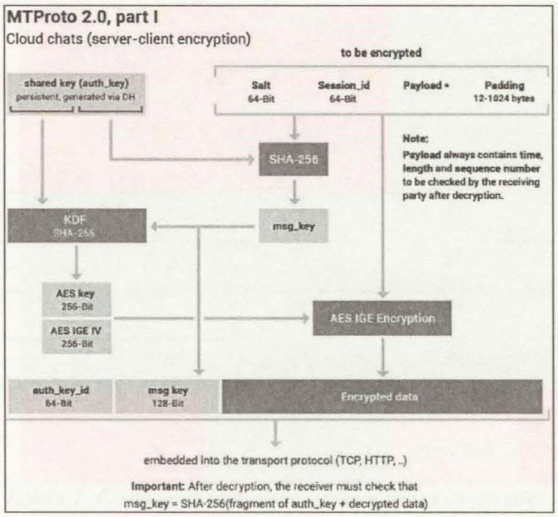


Imagen 8. Estructura del cifrado de Telegram. (247 Tecno, 2017)

Tabla 1. Comparativa de las Aplicaciones Existentes más Conocidas

FUNCIÓN \ APLICACIÓN	WHATSAPP *FACEBOOK*	TELEGRAM *NICOLÁI Y PÁVEL DÚROV*	SIGNAL *OPEN WHISPER SYSTEM*	CELLCRYPT- *MOBILE HIGH SECURITY*	CRYPTOPHONE *GSMK*
Registro inicial	Número Teléfono	Número Teléfono	Número Teléfono	Correo Electrónico	Correo Electrónico
Acceso a contactos	SI	OPCIONAL	SI	OPCIONAL	OPCIONAL
Chat secreto	NO	SI	NO	NO	NO
Chat cifrado en grupo	NO	NO	SI	SI	SI
Chats	SI	SI	SI	SI	SI
Llamadas	SI	SI	SI	SI	SI
Destrucción de mensajes	NO	Solo Chat secreto	SI	NO	NO
Cifrado extremo a extremo	SI	Solo Chat secreto	SI	SI	SI
Protocolo cifrado	Open Whisper System (OWS)	MTPROTO	Open Whisper System (OWS)	cifrado Mobile Content Protocol (EMCP)	TWOFISH
Código abierto	NO	SI	SI	SI	NO

Almacena metadato	En los servidores de la APP	En los servidores distribuidos en la nube	NO	NO	NO
Borrado del historial	SI	SI	SI	SI	SI
Archivos adjuntos con seguridad	SI	SI	SI	SI	SI
Bloqueo con password	SI	SI	SI	SI	SI
Personalización notificaciones	SI	SI	SI	SI	SI
Bloqueo captura de pantalla	NO	SI	Solo en Android	NO	NO

Tabla 1. Comparación entre aplicaciones existentes.

3. Vulnerabilidades presentes en las comunicaciones de telefonía móvil Celular.

Las comunicaciones móviles han venido evolucionando y se han caracterizado por sus avances en tecnología, accesibilidad y disponibilidad al usuario.

Las comunicaciones móviles han tenido sus avances a través de etapas en el transcurso del tiempo, por tal motivo las comunicaciones han tenido 4 generaciones y están distribuidas como se muestra en la Tabla 2.

Tabla 2. Evolución de la comunicación móvil

TECNOLOGÍA	USO	SISTEMA DE COMUNICACIÓN
2G	VOZ	GSM
	DATOS	GPRS-EDGE
3G	VOZ-DATOS	UMTS-HSPA
4G	VOZ-DATO	LTE

Tabla 2. Evolución de la comunicación móvil.

A medida que la tecnología en las comunicaciones móviles ha avanzado, los usuarios también han entrado en el universo de la tecnología móvil, permitiendo a estos tener mayor accesibilidad al mundo de las redes sociales e intercambiar mayor cantidad de información.

Por tal motivo, se puede considerar que la tecnología es directamente proporcional a las vulnerabilidades, por consiguiente, cada evolución de la tecnología móvil tiene sus debilidades que ponen en riesgo la integridad del usuario como se expondrá a continuación:

3.1. Vulnerabilidades en las comunicaciones GSM

3.1.1. Suplantación de usuario

Se llama suplantación cuando la identidad de un móvil es robada para ser usada por un atacante que sustituye al operador de la red móvil realizando llamadas y enviando mensajes de texto en su nombre haciendo que el propietario incurra en el gasto.

La vulnerabilidad se basa en que el atacante puede tener acceso a la identidad del subscriptor móvil temporal (del inglés *Temporary Mobile Subscriber Identity*, en adelante TMSI) y al parámetro Kc[8] a la hora de ser asignada por la red y su autenticación y establecimiento de seguridad.

Una vez el atacante tiene acceso a estos parámetros (TMSI y Ki[9]), estos son introducidos en un firmware para el procesador de banda base para teléfonos GSM el cual implementa las comunicaciones codificadas a través de radios de voz y datos. Por consiguiente, cualquier negociación que se realice en la red ya se encuentra autenticada y el atacante tiene todo el control de la identidad, pudiendo hacer actividades que el propietario no está realizando, a esta amenaza también se puede llamar como clonación de un usuario y se detiene cuando el sistema renueva el TMSI, por lo anterior se puede afirmar que entre más veces la red decida renovar los TMSIs mayor seguridad tendrá el usuario.

[8] Kc: Parámetros de la clave de cifrado.
[9] Ki: Valor individual conocido en SIM y HLR.

3.1.2. Ataques criptográficos

Las comunicaciones GSM incorporan mecanismos de seguridad. Los operadores de red y sus clientes dependen de estos mecanismos para la privacidad de sus llamadas y para la integridad de la red celular. Los mecanismos de seguridad protegen la red mediante la autenticación personalizada en la misma y brindan privacidad a los clientes cifrando las conversaciones mientras se transmiten por el aire.

Hay tres tipos principales de algoritmo criptográfico utilizado en las comunicaciones GSM: A5 se encarga del cifrado de flujo utilizado para el cifrado de las comunicaciones de voz, A3 el algoritmo de autenticación para evitar el clonado de los teléfonos móviles, y A8 El algoritmo de generación de clave para privacidad de voz.

En el 2009 el investigador Karsten Nohl demostró, como se pudo descifrar el algoritmo de A5/1 el cuál se encarga de cifrar las comunicaciones que viajen en el aire. La amenaza empezó cuando el Dr. Nohl realizó una serie de ataques directos a ese algoritmo, que consistía en escuchar la conversación de una víctima por alrededor de 2 minutos y mediante una serie de recursos y herramientas empleados se evidenció que los patrones de cifrado empiezan aparecer en los sistemas empleados, una vez encontrado el patrón, se realiza un barrido de la información almacenada en los discos duros de la máquina empleada y aparece la clave de cifrado de esa conversación permitiendo así al atacante poder descifrar todo el contenido de la conversación, inclusive a los momentos donde no se tuvo acceso mientras se realizaba la búsqueda. (Kalenderi, Pnevmatikatos, Ioannis, & Charalampos, 2012)

3.1.3. Ataque WAP-PUSH y MMS

Este tipo de tecnología permite enviar links que conllevan al usuario a las descargas de malware desde páginas WAP o a contenidos multimedia a través de SMS. Estos enlaces llevan

internamente contenido dañino los cuales están ya configurados para que el usuario del terminal móvil, una vez acepte el mensaje recibido en su bandeja de entrada SMS o MMS, ejecute el contenido malicioso dentro del dispositivo móvil permitiendo al atacante tener el control del terminal.

3.1.4. Ataque de Hombre en el Medio (MITM)

El objetivo de este ataque es la de hacer que el móvil de un usuario se registre en una base creada por un atacante (Base-falsa) permitiéndole así tener el control de las comunicaciones del dispositivo.

Para el desarrollo de este ataque, el atacante debe tener conocimiento de ciertos parámetros del usuario que desea atacar como es la identidad internacional del abonado móvil (en adelante IMSI) generada por el operador que le presta el servicio a la víctima, todos estos datos se encuentran almacenados en la SIM del dispositivo, como se muestra en la Imagen 9.

La idea principal es que el atacante emule una BTS con mayor potencia dentro de la misma frecuencia en la que está localizada la celda y hacer que el móvil de la víctima se autentique con la base falsa y permita que el atacante pueda tener acceso las llamadas realizadas y grabarlas por el dispositivo y capturar el contenido de los mensajes de texto que este realice. (Jose Pico García, 2014)

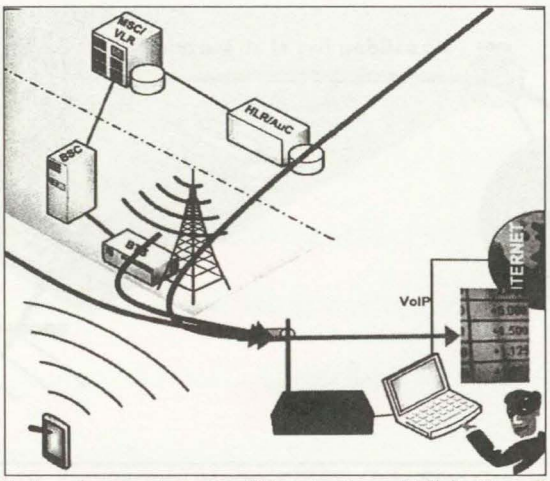


Imagen 9. Ataque de hombre en el medio (Man-in-the-middle). (Jose Pico García, 2014).

3.2. Vulnerabilidad en las comunicaciones GPRS

General Packet Radio Services es un servicio que proporciona acceso de paquetes de radio para el sistema global de comunicaciones móviles (GSM). Permite la provisión de una variedad de aplicaciones y servicios multimedios orientados a paquetes para usuarios móviles, realizando el concepto de Internet móvil, como se puede apreciar en la Imagen 10.

Esta arquitectura se basa en las medidas de seguridad aplicadas a GSM, ya que el sistema GPRS se basa en la infraestructura GSM. Sin embargo, GPRS está más expuesto a intrusos en comparación con GSM porque usa la tecnología IP. Por lo anterior, los intrusos al sistema GPRS pueden intentar violar la confidencialidad, integridad, disponibilidad o intentar abusar del sistema para comprometer los servicios y engañar a los usuarios. (Jose Pico García, 2014).

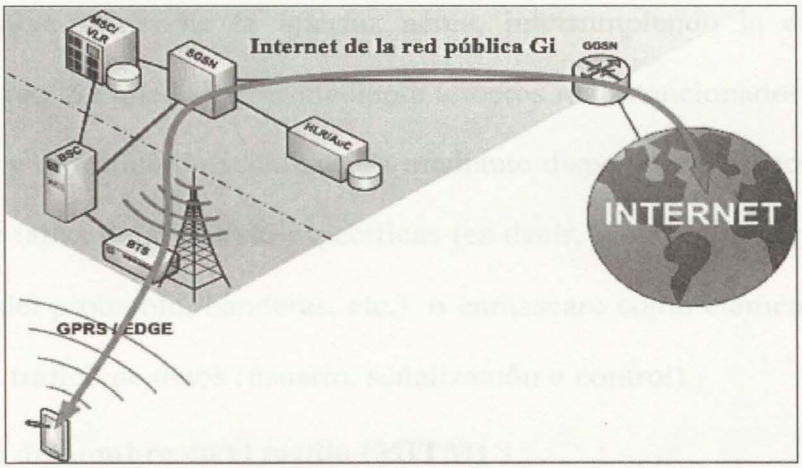


Imagen 10. Arquitectura general GPRS. (Jose Pico García, 2014)

3.2.1. Ataques a la estación móvil (MS)

Los terminales GPRS pueden lidiar con algunas de las mismas amenazas de seguridad que enfrentan las computadoras normales, que están conectadas a la Internet pública. Están amenazados por códigos maliciosos como virus, malware, gusanos, etc., ya que están siempre encendidos y posiblemente estén equipados con un software conocido como navegadores de Internet y aplicaciones de correo electrónico. Los intrusos a las MS pueden modificar, insertar o eliminar aplicaciones o datos almacenados en ellos. Además, el uso de aplicaciones y software inteligentes, que permiten que el código de la computadora se descargue y ejecute en terminales móviles, puede causar varios ataques de seguridad. Los resultados de estos ataques en una MS GPRS pueden ser el monitoreo del uso de MS, la descarga de archivos no deseados, la realización de llamadas de sesión no deseadas, etc., que molestan al usuario final y posiblemente dificultan la ejecución de los servicios solicitados. (Jose Pico García, 2014).

3.2.2. Denegación de servicios

Un ataque común en la interfaz de redes móviles inalámbricas es la denegación de servicio. Este ataque tiene como objetivo prevenir la transmisión de datos de usuario y la información de

señalización y control a través de la interfaz aérea, interrumpiendo la comunicación y el funcionamiento de la red. Se puede lograr mediante terceros malintencionados que: bloqueen los datos de los usuarios y el tráfico de señalización mediante dispositivos especiales denominados bloqueadores, inducir fallas de protocolo específicas (es decir, violar la integridad del protocolo cambiando el estado del protocolo, banderas, etc.); o enmascare como elementos de red y luego evite que se transmita tráfico de datos (usuario, señalización o control).

3.2.3. Ataque de hombre en el medio (MITM)

GPRS es vulnerable a un ataque de hombre en el medio, que permite a un atacante suplantar una estación base falsa a una MS víctima y, al mismo tiempo, suplantar a la víctima a una red real. Se supone que el atacante tiene un dispositivo capaz de emular una estación base, que se integra con una MS y una suscripción de red GPRS válida como se puede apreciar en la Imagen 11.

Este ataque es factible porque la MS está autenticada en la red, pero la red no está autenticada para la MS. Este ataque es posible ya que el atacante obliga a la MS a conectarse a una estación base falsa transmitiendo el código de red de la red doméstica del suscriptor con la mejor calidad de señal. Entonces, la estación base falsa suplanta la MS a la red GPRS. En el proceso de autenticación posterior, el atacante puede simplemente reenviar el tráfico de autenticación entre la MS y la red real, o puede autenticarse en la red utilizando su propia suscripción descartando los datos de autenticación de MS.

Dado que el cifrado entre la MS y la red (SGSN) no es obligatorio y los datos de señalización relacionados se intercambian sin cifrar sin autenticación de origen, el atacante puede solicitar que se desactive el cifrado entre la MS y la estación base falsa.

Por lo tanto, el atacante interviene en la comunicación entre la MS y la red, lo que le permite interceptar, insertar y modificar el tráfico.

Además de la desactivación del proceso de cifrado a través de la interfaz aérea, el ataque de hombre en el medio puede dar como resultado la recuperación de la clave de cifrado utilizada. (Jose Manuel Huidobro Moya, 2006).

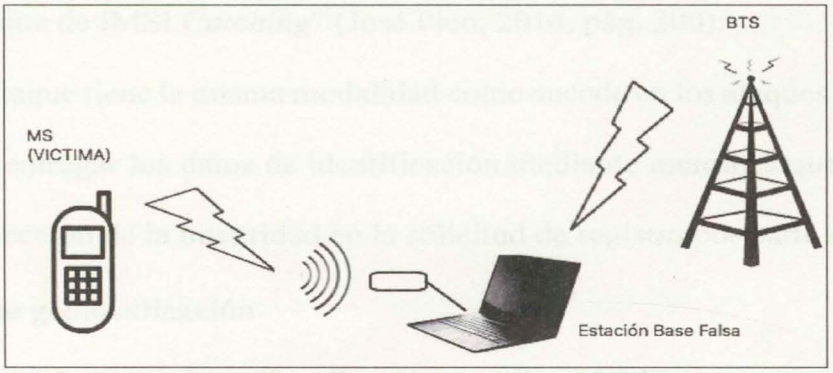


Imagen 11. Ataque Hombre en el Medio (MITM).

3.3. Vulnerabilidades en las comunicaciones UMTS

El sistema de comunicaciones de la tercera generación definido por el grupo del proyecto de asociación de tercera generación (en adelante 3GPP) bautizó a esta nueva tecnología UMTS.

Este sistema maneja estructura de las redes GSM con GPRS como se muestra en la Imagen 12, pero se diferencia a través de los componentes de software.

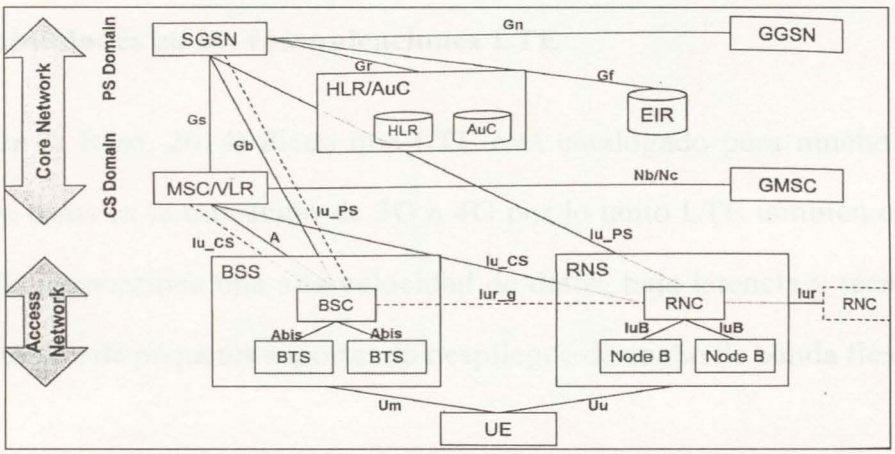


Imagen 12. Arquitectura general UMTS. (Jose Pico García, 2014).

3.3.1. Ataque IMSI catching

Como lo ha señalado José Pico García y David Pérez Conde "La capacidad de determinar la presencia en un área determinada de un dispositivo móvil (conociendo su IMEI o IMSI) es lo que se denomina ataque de IMSI *Catching*" (José Pico, 2014, pág. 200).

Este tipo de ataque tiene la misma modalidad como sucede en los ataques en 2G, la estación base obliga al MS a entregar los datos de identificación mediante mensajes que estén exentos de la obligación de protección de la integridad en la solicitud de registro por parte del móvil.

3.3.2. Ataque geolocalización

Al igual que en el ataque de geolocalización en 2G, en UMTS se realiza de forma similar, con la diferencia que no es posible que el móvil del atacado acepte la solicitud de registro, pero este maneja canales de radio y es de esta manera que se hace posible establecer entre el MS y el nodo-B del RNS[10] para poder realizar los diálogos.

La idea es que el atacante modifique la estación base para que mantenga los canales de radio abiertos el mayor tiempo posible para así, obtener datos para triangular y conseguir la posición del MS.

3.4. Vulnerabilidades en las comunicaciones LTE

(Fernandez & Rizo, 2014) dicen que LTE está catalogado para muchos como la cuarta generación y para otros es la transición de 3G a 4G por lo tanto LTE también es conocida como 3.9 G ya que LTE proporciona una alta velocidad de datos, baja latencia y tecnología de acceso radio con optimización de paquetes soportando despliegue de ancho de banda flexible, velocidades

[10] RNS: Radio Network Subsystem

máximas teóricas de más de 300 Mbps en sentido descendente y 75 Mbps en ascendente, por tal motivo la tecnología LTE se cataloga como 3.9G.

La tecnología LTE fue la evolución de comunicación móvil, que permite una rápida transferencia de grandes cantidades de datos en forma eficiente, rentable y segura como se puede apreciar en su arquitectura de la Imagen 13.

Las redes 3G que se mencionan anteriormente están enfocadas en la transferencia de voz y datos con una velocidad aproximada de acceso de 384 Kbps y máxima o pico de 2 Mbps, velocidad que no es suficiente para proporcionar accesos realmente multimedia.

Las redes 4G/LTE proporcionan una experiencia de banda ancha avanzada con más estabilidad, mayor rendimiento y una menor latencia, alcanzando velocidades de hasta 20 Megas, lo que trae nuevos y mejores servicios para los usuarios.

Dentro de los elementos que forman parte de la arquitectura LTE se encuentran:

- Equipos móviles de usuarios UE.
- Red de acceso evolucionada, E-UTRAN.
- Red troncal de paquetes evolucionada, EPC.

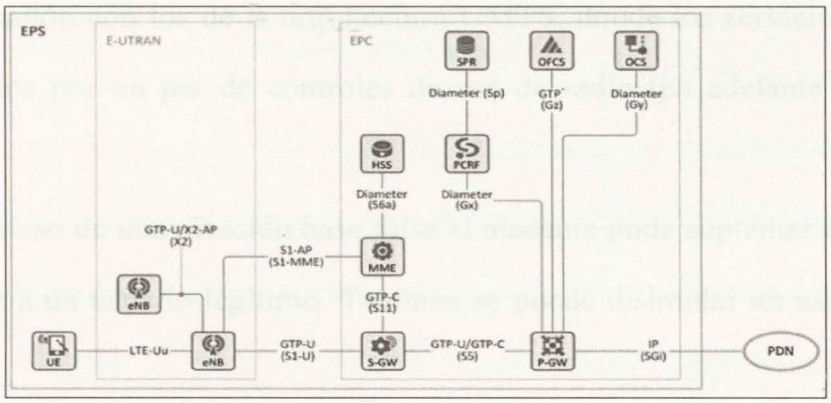


Imagen 13. Arquitectura del sistema LTE. (Muñoz, 2016)

3.4.1. Ataque a la arquitectura LTE

LTE es la primera arquitectura de comunicaciones en transportar todos los datos a través de la conmutación de paquetes (all-IP), incluida la voz por IP, para apoyar las interconexiones con redes de acceso por radio.

La arquitectura basada en all-IP de las redes LTE presentan mayores vulnerabilidades en seguridad como puede ser: inyección, modificación, ataques de escuchas y mayor riesgo de privacidad que en las tecnologías antecesoras como GSM y las redes UMTS. (Griffa, 2007)

A pesar de las capacidades en las comunicaciones 4G ha aumentado, ésta se ha convertido en una arquitectura con mayores vulnerabilidades a los ataques maliciosos tradicionales que se presentan en Internet como el IP *spoofing*[11], ataques de denegación de servicio (DoS), virus, gusanos, correos y llamadas basura etc. (Griffa, 2007).

Existen otras debilidades potenciales causadas por estaciones bases existentes en los sistemas LTE. La red all-IP proporciona un camino directo a las estaciones bases para ataques maliciosos, ya que un área de gestión de movilidad (en adelante MME), gestiona numerosos eNB12 en la arquitectura LTE, las estaciones bases en estas redes son más susceptibles a los ataques en comparación con los de la arquitectura UMTS, donde los servicios de la red UMTS sólo son gestionados por un par de controles de red de radio (en adelante RNC), de manera jerárquica.

Mediante el uso de una estación base falsa el atacante pude suplantar a una estación base genuina para atraer a un usuario legítimo. También se puede disimular un usuario legítimo para

[11] Spoofing: El spoofing es el uso de técnicas de suplantación de identidad generalmente para usos maliciosos.
[12] eNB: Componente de la estación base de la red LTE, que provee la cobertura a los usuarios de ancho de banda móvil.

establecer una conexión con una estación base genuina. Además, dado que el HeNB13 se puede colocar en regiones de la Internet no seguras, es susceptible a un gran número de amenazas de ataques físicos. (Dejun Yang, 2013)

Otro punto vulnerable son los servidores SIP de la red LTE, los cuales no presentan protección IPSec14 y podrían ser un blanco fácil a ataques de hombre en el medio.

Sin embargo, una alternativa que usan los atacantes frente a este tipo de tecnología es la de usar *Smart jamming* o bloqueadores inteligentes que son muy utilizados por los atacantes, debido a su naturaleza sigilosa, hacen que los sistemas de comunicación inalámbricos sean vulnerables ya que pueden aprender rápidamente la potencia de transmisión del usuario y ajustar de forma inteligente su potencia de transmisión para maximizar el efecto dañino (Dejun Yang, 2013). Así como las falsas BTS que también son herramientas muy usadas por los atacantes, ya que esto provoca que el MS que se encuentra en 4G, se baje de tecnología a 3G o 4G y se conecte a la BTS falsa sistema que implementan los atacantes para poder interceptar el trafico de un usuario y se pueda atacar mediante el hombre en el medio como se ha mencionado en anteriores capítulos. (Monowar Hasan, 2013).

3.5. Vulnerabilidades en las comunicaciones 5G

Los avances tecnológicos van a pasos agigantados y en estos momentos se habla del internet de las cosas, y es allí donde entra a jugar la quinta generación que revolucionará las comunicaciones móviles y todo el tratamiento de la información ya que ésta nueva generación será más rápida, más inteligente y consumirá menos energía, lo que permitirá su implementación a

[13] HeNB: realiza la misma función que un eNodeB, pero está optimizado para el despliegue para una cobertura más pequeña que la macro eNodeB, como instalaciones interiores y puntos de acceso públicos.
[14] IPSec: conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet

conectar mayor cantidad de dispositivos inalámbricos como pueden ser los termostatos, sensores, electrodomésticos y vehículos entre otros.

Sin embargo, las pruebas de la implementación de esta tecnología han arrojado una serie de fallas críticas en la confidencialidad de la información, esto presentado por una falla en el protocolo de llaves de arreglo de autenticación (en adelante AKA) que es un mecanismo basado en el proceso de criptografía simétrica.

La vulnerabilidad presentada puede develar la actividad de un usuario, como el número de llamadas y mensajes de texto enviados y recibidos.

En el 2018 un especialista en seguridad David Vignault menciono que "Las actividades de espionaje en áreas estratégicas auspiciadas por agencias gubernamentales han incrementado, igualmente en los sectores sensibles, como la investigación en inteligencia artificial, fármacos y tecnología militar, podría verse severamente afectada por esta clase de fallas de seguridad en los protocolos de comunicación móvil".

3.6. Vulnerabilidad en los diferentes sistemas operativos móviles

El sistema operativo es el encargado de gestionar el funcionamiento del hardware del equipo móvil mediante el empleo de herramientas de software que controlan un dispositivo móvil, el cual está orientada a la conectividad inalámbrica, la administración de forma óptima del procesamiento, almacenamiento y el consumo de la energía, entre otras.

Los sistemas operativos móviles cuentan con capas específicas, la capa del Kernel o núcleo del sistema operativo encargado de administrar todos los elementos de hardware del dispositivo móvil, la capa del Middleware o intermediador de aplicaciones del sistema operativo, son diferentes programas o módulos que permiten el uso de aplicaciones, librerías, entre otras para el funcionamiento del dispositivo móvil, la capa de administración de aplicaciones que es la

encargada de la ejecución, detención y finalización de las aplicaciones del sistema operativo y por último la capa interfaz la cual es la encargada de administrar el uso que le da el usuario al dispositivo móvil ya sea de pantalla táctil.

Los dispositivos móviles cuentan con unas características básicas en su interior y especificaciones como las siguientes:

- Debe poseer un Kernel
- Se encuentra construido por capas.
- Deben ser de multiproceso y multitarea.
- Debe soportar diferentes pantallas.
- Debe soportar el multi-lenguaje.
- Conexión inalámbrica.
- Debe administrar el hardware.
- Navegación web.
- Debe administrar las aplicaciones.

Dentro de la familia de los sistemas operativos y durante el desarrollo de este trabajo solo se hará énfasis en los sistemas operativos (Android y IOS), que se describirán a continuación.

Android: Es el sistema operativo más versátil y libre que ha ido ganando terreno a lo largo de los fabricantes de dispositivos móviles. La filosofía de Android es la de tener un entorno abierto que sea manipulable a gusto por cualquier programador y fabricante a modo de distribuirlo a los usuarios.

Como aspecto negativo, Android al ser versátil y flexible y según la empresa de seguridad informática ESET las vulnerabilidades de dispositivos con este sistema operativo en el 2017 fue del 87,7%, esto lo convierte en una plataforma que posee muchas vulnerabilidades relacionadas

con aspectos de seguridad, ya que serán blanco de atacantes debido al flujo de la información que muchas personas manejan (Bartolomé, 2018).

ATAQUES: Las aplicaciones que se desarrollan para este sistema operativo, hacen más vulnerable la resistencia a los códigos maliciosos, que exponen a millones de usuarios a riesgos importantes al utilizar sus terminales, un informe de Nokia asegura que la cantidad de infecciones ha aumentado considerablemente en 2016, siendo el 81% de los dispositivos infectados pertenecientes a Android, y por parte de Laboratorio de investigación de ESET Latinoamérica, los fallos de seguridad de dispositivos con este sistema operativo en el 2017 fue del 40,5%. (Luque, 2017)

Una de las herramientas más útiles para los delincuentes informáticos es el mismo usuario ya que este permite que los delincuentes accedan a la información mediante la aceptación de aplicaciones de desarrolladores desconocidos. Como por ejemplo un ataque que está de moda son los Ransomware[15] que consiste en que un delincuente cifra la información del dispositivo, solicitando un alta suma de dinero para descifrarla y por otra parte el phishing[16] que permite al atacante insertar un malware y poder descubrir claves y códigos personales como lo puede ser la clave de la cuenta del banco.

IOS: Es el sistema operativo que solo usan los dispositivos IPhone y el IPad, según las estadísticas de *NetMarketShare*, el uso de dispositivos con este sistema operativo en el 2017 fue del 40,5% y es un dispositivo con un muy buen rendimiento, intuitivo, y es sencillo de manejar, lo que muchos usuarios critican es que, a diferencia de Android, IOS es cerrado y muchas veces es

[15] Ransomwae: software malicioso que restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción

[16] Phishing: es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

incómodo el instalar aplicaciones que no sean de ellos. Pero eso lo puede convertir en un dispositivo un poco más seguros contra ataques.

ATAQUES: Si bien el uso de dispositivos móviles con sistemas operativos IOS es del 12% del mercado según Laboratorio de investigación de ESET Latinoamérica, ubicándolo como el segundo competidor con mayor cantidad de dispositivos empleado por usuarios, debido a su aparente seguridad que el dispositivo presenta.

Lo último en seguridad para la empresa Apple, fue la actualización de la versión IOS 11, el cuál incluyó mejoras de seguridad que permitieron fortalecer los procesos de autenticación en esta plataforma. Sin embargo, las vulnerabilidades que presentan estos sistemas han aumentado, por ejemplo, si una persona se ausenta por unos minutos y olvida el teléfono un atacante puede tomar ventaja de algo de información importante, sin tener que robar el dispositivo (Alonso C., 2013, pág. 23).

En el caso de este sistema operativo se publicaron 365 vulnerabilidades en 2017, 126.71 veces más que la cantidad encontrada en 2016 y prácticamente la mitad de las identificadas en Android durante ese mismo período.

Dentro de las amenazas más comunes en este sistema operativo se encuentran: los malware y los *ramsomware*, al igual que en los sistemas operativos Android y esto es debido al incremento del uso de estos dispositivos en el mundo.

A modo de conclusión del capítulo, en la Tabla 3, se relacionan los ataques en cada una de las evoluciones de la tecnología móvil celular.

Tabla 3. Ataques según tecnologías de telefonía móvil celular

TECNOLOGÍA	ATAQUES
GSM	Suplantación de usuario, ataques criptográficos, ataque Wap-Push y MMS, Ataque de hombre en el medio (MITM).
GPRS	Ataque a estación móvil, denegación de servicio, ataque MITM, ataque red principal GPRS, ataque a la interfaz de internet de la red pública.
UMTS	Ataque IMSI Catching, ataque de geolocalización, ataque de denegación de servicio
LTE	Ataque en el proceso de Handover en LTE, Vulnerabilidad en el mecanismo de seguridad en HeNB

Tabla 3. Ataques presentes en las diferentes tecnologías de telefonía móvil celular.

4. Análisis del riesgo asociado a las vulnerabilidades presentes en las comunicaciones móvil celular

Las redes móviles celulares presentan vulnerabilidades importantes que comprometen la seguridad de la propia red, así como la seguridad en las comunicaciones y la información de los usuarios, de ahí la importancia de buscar soluciones de seguridad para el uso seguro de la telefonía móvil.

Según Owasp (Owasp, 2017), en la última actualización de vulnerabilidades móviles 2016, describe las amenazas de seguridad como se muestra en la tabla 4 "Mobile top 10 2016" así:

Tabla 4. Vulnerabilidades móviles OWASP 2017

M1	Uso inapropiado de las plataformas	Esta categoría cubre el uso indebido de una característica de la plataforma o la imposibilidad de utilizar los controles de seguridad de la plataforma. Puede incluir intenciones de Android, permisos de plataforma, mal uso del TouchID, el llavero o algún otro control de seguridad que sea parte del sistema operativo móvil. Hay varias formas en que las aplicaciones móviles pueden experimentar este riesgo.
M2	Almacenamiento inseguro de la información	Esta nueva categoría es una combinación de M2+ M4 de Mobile Top Ten 2014. Esto abarca el almacenamiento de datos inseguros y la fuga de datos involuntarios.
M3	Comunicaciones inseguras	Esto incluye mala comunicación, versiones incorrectas de SSL, negociación débil, comunicación clara de activos confidenciales, etc.
M4	Autenticaciones inseguras	Esta categoría capta nociones de autenticación del usuario final o gestión de sesión incorrecta. Esto puede incluir: • No identificar al usuario en absoluto cuando eso debería ser requerido • No mantener la identidad del usuario cuando se requiere • Debilidades en la gestión de sesiones
M5	Criptografía insegura	El código aplica criptografía a un activo de información sensible. Sin embargo, la criptografía es insuficiente de alguna manera. Tenga en cuenta que todo lo

		relacionado con TLS o SSL va en M3. Además, si la aplicación no puede usar la criptografía cuando debería, eso probablemente pertenece a M2. Esta categoría es para los problemas donde se intentó la criptografía, pero no se realizó correctamente.
M6	Autorización insegura	Esta es una categoría para capturar cualquier falla en la autorización (por ejemplo, decisiones de autorización en el lado del cliente, navegación forzada, etc.). Es distinto de los problemas de autenticación (por ejemplo, inscripción del dispositivo, identificación del usuario, etc.). Si la aplicación no autentica a los usuarios en una situación en la que debería (por ejemplo, otorgar acceso anónimo a algún recurso o servicio cuando se autentica y se requiere acceso autorizado), entonces se trata de una falla de autenticación y no de una autorización
M7	Calidad del código del cliente	Esta fue la "Decisiones de seguridad a través de insumos no confiables", una de nuestras categorías menos utilizadas. Esta sería la solución para los problemas de implementación a nivel de código en el cliente móvil. Eso es distinto de los errores de codificación del lado del servidor. Esto capturaría cosas como desbordamientos de búfer, vulnerabilidades de cadena de formato y varios otros errores de nivel de código donde la solución es reescribir algún código que se ejecuta en el dispositivo móvil.
M8	Alteraciones del código	Esta categoría cubre el parche binario, la modificación de recursos locales, el enganche de métodos, el swizzling de métodos y la modificación de memoria dinámica. Una vez que la aplicación se entrega al dispositivo móvil, el código y los recursos de datos residen allí. Un atacante puede modificar directamente el código, cambiar los contenidos de la memoria de forma dinámica, cambiar o reemplazar las API del sistema que utiliza la aplicación o modificar los datos y recursos de la aplicación. Esto puede proporcionar al atacante un método directo para subvertir el uso previsto del software para obtener ganancias personales o monetarias.
M9	Ingeniería inversa	Esta categoría incluye el análisis del núcleo binario final para determinar su código fuente, bibliotecas, algoritmos y otros activos. Software como IDA Pro, Hopper, otool y otras herramientas de inspección binaria le dan al atacante una idea del funcionamiento interno de la aplicación. Esto se puede usar para explotar otras vulnerabilidades incipientes en la aplicación, así como también para revelar información acerca de los servidores back-end, las constantes cifrados criptográficos y la propiedad intelectual.
M10	Funcionalidad extraña	A menudo, los desarrolladores incluyen funciones ocultas de puerta trasera u otros controles internos de seguridad de desarrollo que no están destinados a ser lanzados a un entorno de producción. Por ejemplo, un desarrollador puede incluir accidentalmente una contraseña como comentario en una aplicación híbrida. Otro ejemplo incluye la desactivación de la autenticación de 2 factores durante la prueba.

Tabla 4. Vulnerabilidades móviles OWASP. (Owasp, 2017).

4.1. Medidas a implementar por el operador móvil

Las actualizaciones que han tenido las redes LTE por parte de los operadores de telefonía móvil no han sido suficientes para mitigar las vulnerabilidades ya que éstas presentan fallas de seguridad que pueden ser empleadas para engaños y ataques, por lo que es necesario suministrar soluciones para mitigar la seguridad por parte del operador y del usuario (abonado).

Por parte del usuario se debe manejar la seguridad de su dispositivo móvil, y por parte del operador se deben mejorar ciertas áreas de la infraestructura así:

4.1.1. Creación de la lista negra

La lista negra es creada por el operador de red, la cual posee una lista de números de serie electrónica de SIM o equipo de teléfono celular que se han reportado como perdidos o robados.

4.1.2. Almacenamiento de la información

Para proteger la confidencialidad de la información almacenada en los dispositivos móviles, se recomienda emplear mecanismos de cifrado de los datos. La solución de cifrado debe ser aplicada tanto a las capacidades de almacenamiento internas del dispositivo, como a las tarjetas de memoria externas, debido a la movilidad asociada a ambos tipos de almacenamiento y su exposición a intrusos potencialmente interesados en los datos almacenados.

Es posible emplear software de cifrado independiente del sistema operativo del dispositivo y que sólo protege ciertos datos. Para acceder a los datos protegidos por este software es necesario disponer de una contraseña, independiente del código de acceso al dispositivo, que permite gestionar la información más confidencial (Centro Criptologico Nacional, 2013).

4.1.3. Buenas prácticas de uso seguro de la telefonía móvil por parte de usuario.

Las buenas prácticas de las comunicaciones móviles se crean mediante estándares dictados por cada país, en Colombia estos estándares son establecidos por la CRC (la comisión de Regulación de Comunicaciones), ISO 9001 - SC 1390-1, MINTIC (Ministerio de la Tecnología de la Información), la ANE (Agencia Nacional del Espectro). (Germán Darío Arias Pimiento, 2016)

Lo primero que se debe hacer es asumir que las conversaciones de voz a través de dispositivos móviles no son confidenciales, al igual que no lo son otros medios de comunicación como el fax o e-mail, pese al carácter cerrado de la infraestructura de la telefonía móvil.

La recepción de mensajes de texto SMS es el objetivo de múltiples ataques, por lo que se recomienda no abrir ningún mensaje de texto no esperado o solicitado y sea cuidadoso con las

descargas de software, correos electrónicos, mensajes del sistema o cualquier otro evento de este tipo que no haya sido solicitado.

En cuanto a la seguridad asociada a las comunicaciones de datos a través de las infraestructuras de telefonía móvil en dispositivos móviles se recomienda no activar las capacidades de transmisión y recepción de datos salvo en el caso en el que se esté haciendo uso de éstas, evitando así la posibilidad de ataques sobre el hardware del interfaz, el controlador, la pila de comunicaciones móviles y cualquiera de los servicios y aplicaciones disponibles a través de esa red y la conexión a Internet.

5. Modelo tecnológico que permita asegurar las comunicaciones estratégicas del Estado

En los capítulos anteriores se han podido apreciar las vulnerabilidades que tienen las comunicaciones móviles actualmente y como se pueden analizar éstas para mitigar el riesgo.

Sin embargo, las soluciones mencionadas en el capítulo 2 no garantizan un 100 por ciento la seguridad en las comunicaciones de altos funcionarios del Estado, ya que las aplicaciones que son libres no cumplen con las medidas de seguridad como acceso a contactos, no han develado el código, no cuentan con chat secreto, almacenan metadatos como se muestra en la tabla 3 y las que son de pago son muy costosas y almacenan en los servidores de los proveedores la información que por esta pasa.

Por lo anterior, es de vital importancia que los altos funcionarios del Estado Colombiano cuenten con un sistema de comunicación segura que permita transmitir información confidencial sin tener ningún riesgo que exista una fuga de información. Debido a eso hay una necesidad de implementar una plataforma que brinde seguridad a las comunicaciones estratégicas a través de los dispositivos de telefonía móvil celular, enfoque que se presenta en este trabajo de grado.

5.1. Identificación de la necesidad

- Para el desarrollo del presente trabajo fue necesario identificar primero que funcionarios son considerados del alto gobierno, ya que no todos los funcionarios tienen comunicaciones estratégicas de estado.
- Elaborar el modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móvil celular.

5.1.1. Identificación de los funcionarios

Para el presente modelo se considera importante conocer quiénes son los funcionarios que utilizarán la herramienta, según la página de la presidencia (Presidencia de la República, 2018), las personas a las que estaría dirigido el modelo propuesto son:

- El presidente de la Republica
- El vicepresidente de la República
- 16 ministros
- 13 asesores
- Comandante de las fuerzas Militares
- Comandante de la policía

5.2. Desarrollo del modelo de comunicación segura

El modelo que se describe a continuación se basó en los parámetros del número de funcionarios que van a implementar el modelo, que para este caso se desarrollará para 50 funcionarios. Si bien el modelo es escalable para n número de funcionarios el objetivo inicial es la de asegurar las comunicaciones estratégicas de Estado, y en principio los funcionarios anteriormente mencionados son quienes en primera instancia tienen comunicación directa en la

toma de decisiones estratégicas del Estado.

El modelo que se desarrolla se basa en los 8 principios básicos de la seguridad de la información según la recomendación de la UIT-T X.805. (UIT, 2004, pág. 9) donde la arquitectura de seguridad UIT-T X.805 es una referencia para definir políticas de seguridad globales, planes de emergencia ante incidentes, recuperación y arquitectura tecnológica.

Los 8 principios de seguridad de la información de la UIT-T X.805 en el que se basa el modelo son:

- **Control de acceso**: Este servicio se emplea para evitar el uso no autorizado de recursos y que solo las personas y dispositivos autorizados puedan acceder a los elementos de red, información almacenada, los servicios y las aplicaciones.
- **Autenticación**: Este servicio autentica la identidad de las fuentes que tratan de comunicarse, es decir se garantiza la aprobación de la identidad que se le ha atribuido a las fuentes de una comunicación bien sean personas o dispositivos.
- **No repudio**: El no repudio ofrece protección a un usuario o entidad frente a que otro usuario niegue posteriormente que en realidad hubo un tratamiento de datos.
- **Confidencialidad**: La confidencialidad asegura que la información sensible solo podrá ser consultada o manipulada por usuarios, entidades o procesos autorizados.
- **Integridad**: La integridad de los datos garantiza la exactitud y la veracidad de los datos. No permite acciones no autorizadas de modificación y eliminación de estos.
- **Disponibilidad**: La disponibilidad garantiza que la infraestructura de la red no impida el acceso autorizado a los elementos de esta como es la información almacenada, los flujos de información, los servicios y las aplicaciones.

- **Privacidad**: La privacidad protege la información de que terceros puedan conocer las actividades que los usuarios están realizando en la red, por ejemplo, poder conocer la dirección IP, o la MAC de un dispositivo que se encuentre haciendo una actividad.
- **Seguridad en la comunicación**: La seguridad en la comunicación permite que la información tenga un flujo desde los puntos autorizados desde donde inicia hasta donde termina sin que tenga ninguna interrupción. Por ejemplo, que no se pueda interceptar.

El modelo general que se implementará en este trabajo de grado es el que se puede apreciar en la Imagen 14.

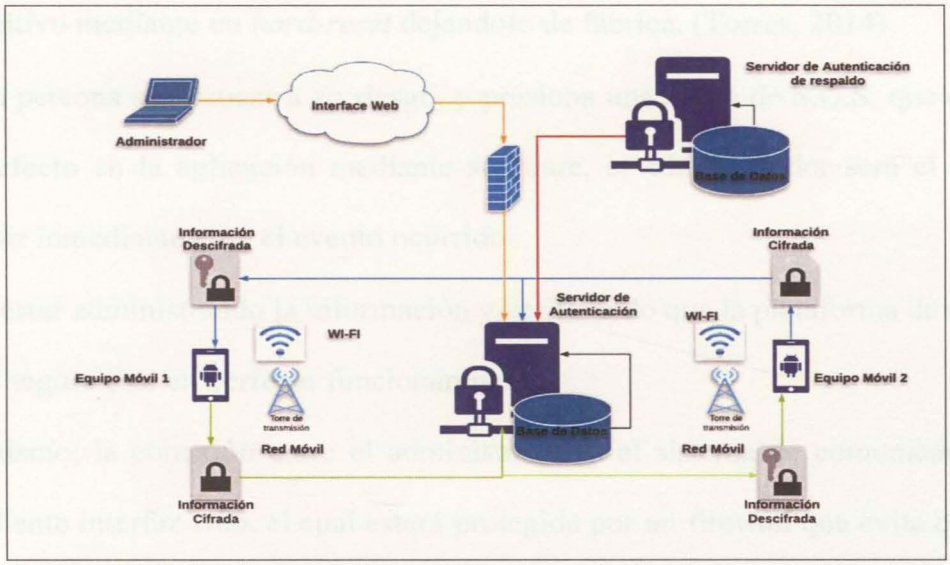


Imagen 14. Modelo general de la plataforma tecnológica que brinda seguridad a las comunicaciones estratégicas del Estado.

Para el desarrollo de este modelo estará dividido en 3 módulos:

- Módulo de administración.
- Módulo de enlace, almacenamiento y autenticación.
- Módulo de software de aplicación.

5.2.1. Módulo de administrador

Este módulo se centra en el usuario administrador que tendrá el control de la verificación y de constatar que el sistema se encuentra en perfecto funcionamiento como se muestra en la Imagen 15, dentro de las funciones del administrador del sistema se encuentran:

- Verificar el funcionamiento del sistema.
- Si un dispositivo se extravía, el administrador es el encargado de realizar la búsqueda de este mediante la aplicación de geolocalización y de borrar la información (*wipe*), es decir que mediante software el administrador podrá eliminar remotamente el contenido del dispositivo mediante un *hard-reset* dejándolo de fábrica. (Torres, 2014)
- Si una persona se encuentra en riesgo, y presiona una alerta de S.O.S, que se establecerá por defecto en la aplicación mediante software, el administrador será el encargado de reportar inmediatamente el evento ocurrido.
- Debe estar administrando la información y verificando que la plataforma de comunicación móvil segura esté en perfecto funcionamiento.

Así mismo, la conexión entre el administrador y el sistema de comunicación móvil se realizará mediante interfaz web, el cual estará protegida por un firewall que evita que se generen vulnerabilidades en la red de acceso.

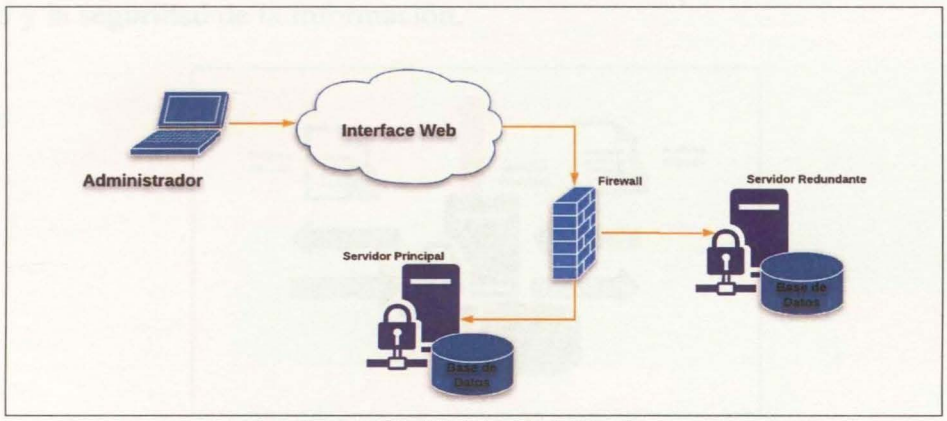


Imagen 15. Módulo Administrador

5.2.2. Módulo de enlace, almacenamiento y autenticación

Este módulo se encarga de realizar el enlace de la comunicación a través del servidor y a su vez permite almacenar la información dejando la trazabilidad de los usuarios como se puede apreciar en la Imagen 16.

Si se realiza una transmisión por texto, el dispositivo móvil 1 escribe el mensaje lo cifra lo envía al servidor, el servidor lo recibe y verifica si este pertenece a la base de datos y lo envía tal cual, cifrado al dispositivo móvil 2 y este lo descifra, si la llave de cifrado es la misma el mensaje coincide con el que envió del dispositivo móvil 1 de lo contrario llegara un texto que no corresponde al mensaje.

Si se realiza una transmisión de voz, el enlace de la comunicación que se efectúa a través del servidor es diferente, si se quiere generar una llamada del dispositivo móvil 1 al dispositivo móvil 2, el dispositivo móvil 1 llama, le avisa al servidor que se va a comunicar, el servidor le indica al dispositivo móvil 2 que está recibiendo una llamada, el dispositivo móvil 2 empieza a timbrar, cuando se contesta la llamada, el dispositivo móvil 2 le avisa al servidor que acepta la llamada y el servidor le avisa al dispositivo móvil 1 y se genera la comunicación cifrada.

Así mismo, la información que se esté almacenando en el servidor principal estará automáticamente quedando almacenada en el servidor de respaldo, proporcionando así la disponibilidad y la seguridad de la información.

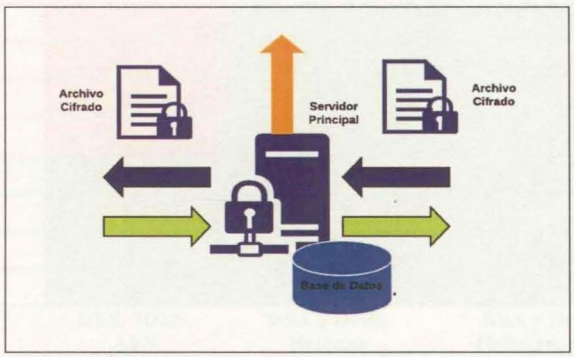


Imagen 16. Módulo de enlace, almacenamiento y autenticación

- **Modo de Autenticación**

En esta parte se centra la importancia de la seguridad de la información ya que por este medio se procesa el cifrado de la misma. Actualmente hay 3 formas básicas de cifrado conocidas como lo es cifrado simétrico, cifrado asimétrico e infraestructura de llave pública (del inglés *Public Key Infraestructure*, en adelante PKI).

  - **Cifrado simétrico:** es un sistema criptográfico en el que el emisor y receptor emplean las mismas claves para el cifrado y el descifrado
  - **Cifrado asimétrico:** el sistema criptográfico asimétrico emplea 2 tipos de claves; una llamada clave pública y otra llamada clave privada, las claves públicas son conocidos por todos los actores y las claves privadas siempre se mantendrán en secreto por cada actor.
  - **Cifrado PKI:** el sistema de cifrado de las infraestructuras de llave pública consiste en autenticarse frente a otro usuario gestionando los certificados de clave pública.

En la tabla 5, se puede apreciar una comparación entre los cuatro sistemas de cifrado como lo son: cifrado simétrico, cifrado asimétrico, cifrado híbrido y cifrado PKI, donde se puede ver que el sistema óptimo a implementar en el presente modelo es el cifrado asimétrico y el modelo híbrido.

Tabla 5. Comparación

	Cifrado Simétrico	Cifrado Asimétrico	Cifrado simétrico + Asimétrico (Híbrido)	Cifrado PKI
Autenticación				
No repudio				
Confidencialidad				
Integridad				
Disponibilidad				
Privacidad				
Factor económico				
Esçalabilidad				
Algoritmos	DES, 3DES, AES	RSA y Deffie Hellman	RSA y Deffie Hellman, AES	Hash

Tabla 5.Comparación entre los sistemas de cifrado.

Por lo anterior, la investigación arrojo que, el cifrado que mejor se adapta al modelo expuesto en este trabajo de grado es el cifrado híbrido el cual se muestra en la Imagen 17. (UIT-T, 2006).

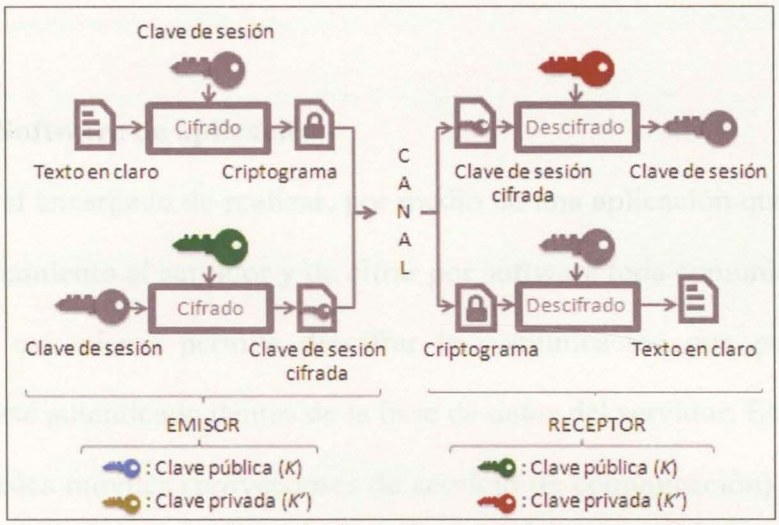


Imagen 17. Proceso de cifrado híbrido con firma digital. (Larragan, 2016)

El procedimiento del cifrado híbrido que se empleara para el envío de la información se describe a continuación:

1. La información se cifra con cifrado simétrico mediante una clave simétrica aleatoria, generalmente de 128/256 bits.
2. Se consigue la clave pública del receptor en un directorio que estará disponible en el servidor, generalmente, la clave pública tiene 1024bits.
3. Se cifra la clave simétrica con la clave pública del receptor: "Operación de clave empaquetada".
4. Se crea un sobre digital que contiene la clave simétrica cifrada y el texto cifrado con la clave simétrica.
5. Se envía el sobre digital

6. El receptor abre el sobre, encuentra el texto cifrado y la clave empaquetada.
7. El receptor con su clave privada descifra la clave empaquetada.
8. Ahora, el receptor descifra la información cifrada y lo convierte en claro con la clave simétrica.

5.2.3. Módulo Software de aplicación

Este módulo es el encargado de realizar, por medio de una aplicación que se instala en el dispositivo, el direccionamiento al servidor y de cifrar por software toda comunicación que salga a través del terminal, así mismo permite descifrar la comunicación que provenga de otro dispositivo móvil que esté autenticado dentro de la base de datos del servidor. Esta comunicación se realiza a través de redes móviles (proveedores de servicio de comunicación), y/o redes wi-fi, como se representa en la imagen 18.

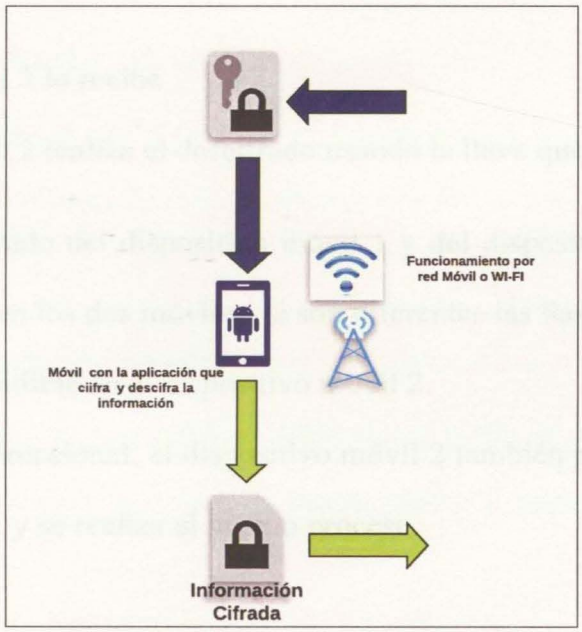


Imagen 18. Módulo de software de aplicación

5.2.4. Descripción del Funcionamiento del sistema

- **Proceso de comunicación**

1. Inicializar las aplicaciones en los dos celulares, estos piden conexión a los puertos del servidor designados por el administrador
2. Se establece la comunicación entre los dos celulares y el servidor.

Transmisión de mensajes de texto:

1. Se escribe un mensaje en el dispositivo móvil 1, el software de la aplicación define una llave de cifrado.
2. El mensaje se cifra por medio de la llave.
3. Se transmite el mensaje del celular al servidor.
4. El servidor lo recibe y transmite el mismo mensaje (el cual va encriptado) al dispositivo móvil 2.
5. El dispositivo móvil 2 lo recibe
6. El dispositivo móvil 2 realiza el descifrado usando la llave que tiene en este dispositivo.

Si las llaves de cifrado del dispositivo móvil 1 y del dispositivo móvil 2 son iguales el mensaje se visualiza igual en los dos móviles, si son diferentes las llaves de cifrado el mensaje se va a ver cambiado e inentendible en el dispositivo móvil 2.

Este proceso es bidireccional, el dispositivo móvil 2 también puede enviar un mensaje de texto al dispositivo móvil 1 y se realiza el mismo proceso.

Comunicación de Voz

1. En el dispositivo móvil 1 genera una llamada al dispositivo móvil 2.
2. El dispositivo móvil 1 envía un mensaje con la solicitud de llamada, cifrando la solicitud.
3. El servidor recibe la solicitud.

4. El servidor autentica y envía al dispositivo móvil 2 la solicitud.
5. El dispositivo móvil 2 recibe le mensaje y lo descifra usando la llave que tiene designada en el móvil.
6. Si el mensaje después de descifrar corresponde al mensaje de solicitud de llamada, genera el timbre de llamada.
7. Si el usuario decide contestar la llamada presiona el botón contestar.
8. Se envía del dispositivo móvil 2 al servidor la solicitud de contestar de manera cifrada.
9. El dispositivo móvil 2 inicializa la comunicación por uno de sus sockets y se queda en modo de escucha.
10. El servidor recibe la solicitud y la envía al dispositivo móvil 1.
11. El dispositivo móvil 1 recibe la solicitud y lo descifra, si corresponde a un mensaje valido, Inicializa el socket y envía una comunicación por este puerto para establecer la comunicación entre los dos celulares.
12. Los dos celulares quedan conectados por el mismo socket.
13. Se transmite el audio empaquetado y cifrado con la llave que está en el software de la aplicación.

Si las llaves de cifrado son iguales en los dos dispositivos el audio que se genera en un celular se oye igual en el otro, si las llaves son diferentes el audio no va a ser el mismo.

Este proceso es bidireccional, el dispositivo móvil 2 también puede enviar audio al dispositivo móvil 1 realizando el mismo proceso.

Por lo anterior, es de importante resaltar que mientras que se realiza la comunicación entre los dos dispositivos móviles, el servidor va almacenando toda la información que esta ocurriendo

en ese momento como: la fecha, hora, dispositivos que se comunica y el mensaje de texto o la conversación de voz.

De igual manera se puede identificar que el modelo de plataforma tecnológica que se presenta en este trabajo debe ser escalable, a medida que crezca el número de usuarios que necesiten usar la plataforma, esta escalabilidad se verá reflejada en el aumento de la cantidad de servidores o de la adquisición de servidores más potentes aumentando el número de canales al exterior con mayor potencia, la capacidad de usuarios depende directamente de la potencia de los servidores del canal de comunicación y el almacenamiento que permitan la interconexión entre los dispositivos móviles. Así como aumentar la disponibilidad del almacenamiento de los servidores redundantes que estarán almacenando alternamente la información como lo dice la norma ISO 27001.

Lo anterior se puede ver resumido en los diagramas de caso de uso de la imagen 19 y 20.

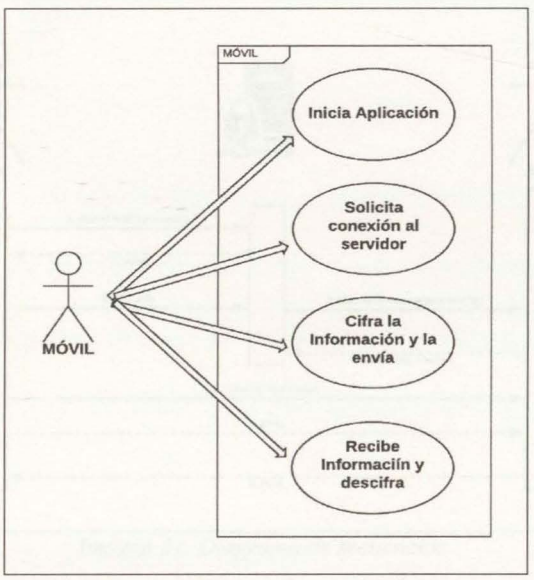


Imagen 19. Diagrama de caso de uso del dispositivo móvil.

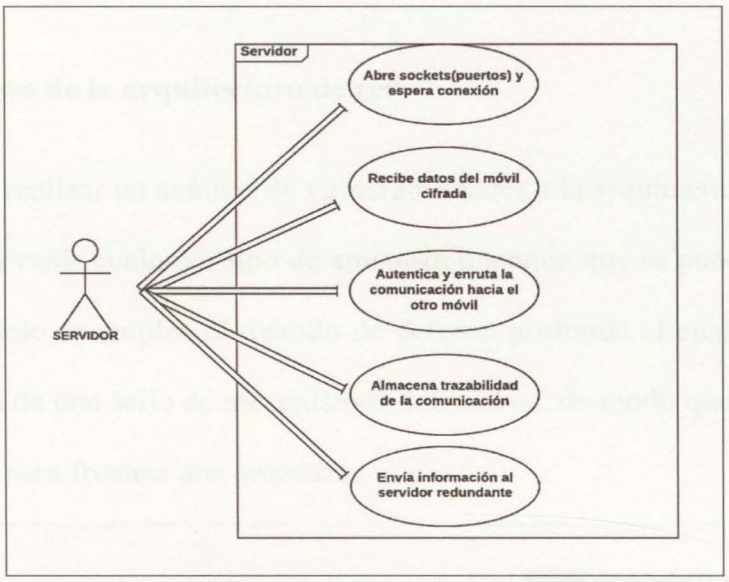


Imagen 20. Diagrama de caso de uso del servidor

En la imagen 21, se puede apreciar el diagrama de uso para el modelo propuesto, donde se relacionan las actividades que realizarán los usuarios del sistema.

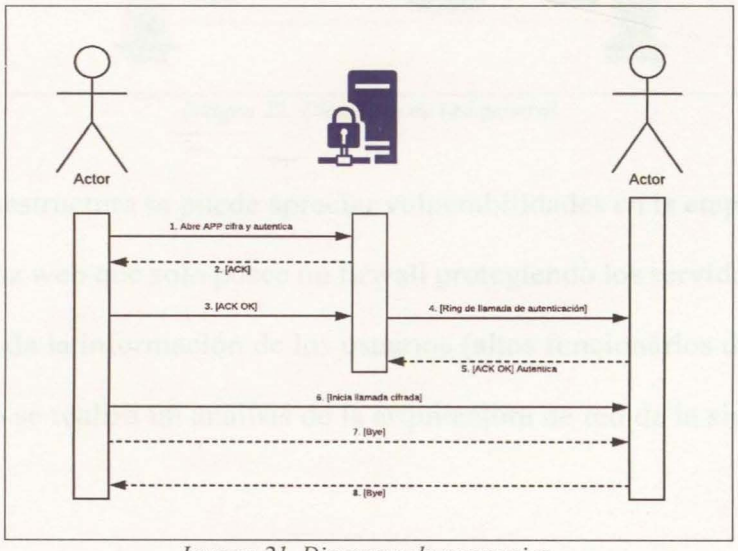
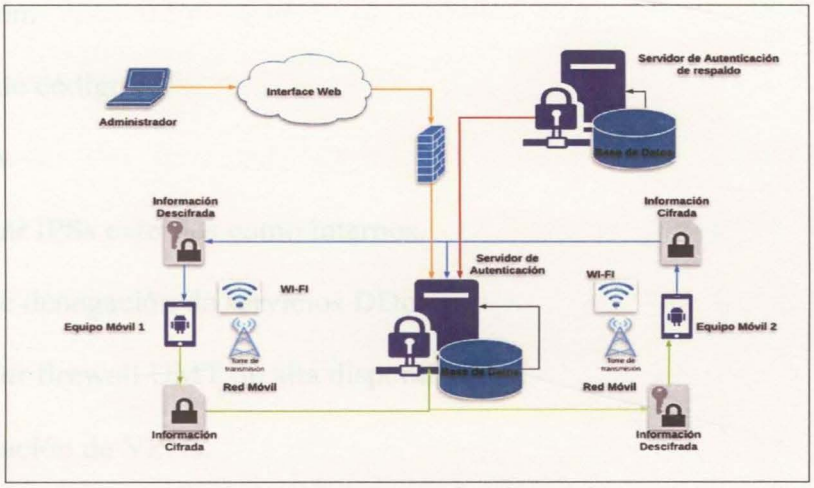


Imagen 21. Diagrama de secuencias.

5.3. Aseguramiento de la arquitectura de red

Es importante realizar un análisis de vulnerabilidades a la arquitectura de red propuesta en la imagen 22, para prevenir cualquier tipo de amenaza o ataque que se pueda producir a nivel de infraestructura, para esto se emplea el método de defensa profunda el cual permitirá proteger la red propuesta a través de una serie de mecanismos defensivos, de modo que, si uno de estos falla, otro ya está instalado para frustrar una amenaza.



Imágen 22. Diagrama de red general.

Para esta infraestructura se puede apreciar vulnerabilidades en la etapa de administrador ya que esta es una interfaz web que solo posee un firwall protegiendo los servidores y la base de datos donde se encuentra toda la información de los usuarios (altos funcionarios del Estado).

Por tal motivo se realiza un análisis de la arquitectura de red de la siguiente manera:

5.3.1. Análisis sobre la capa de Perímetro

Hallazgos

- No existen controles a nivel de aplicación web.

- No existe solución a la detección de intrusos IPS.
- No existe seguridad en los accesos al sistema.
- No existe una conexión segura entre el administrador y los servidores.
- Existe vulnerabilidad en la base de datos principal como en la base de datos alterna.

Riesgos identificados

- Denegaciones de servicio.
- Ataques a las bases de datos.
- Suplantación.
- Inyección de código.

Recomendaciones

- Implementar IPSs externos como internos.
- Sensores de denegación de servicios DDos.
- Implementar firewall UMT de alta disponibilidad.
- Implementación de VPNs.

5.3.2. Análisis sobre la capa de Host

Hallazgos

- No existe una protección para el acceso no autorizado.
- No hay una mitigación de denegación de servicio
- No existe una política de desarrollo seguro

Riesgos identificados

- Ingreso a la red sin autorización.
- Ataques a las bases de datos.

- Suplantación.

Recomendaciones

- Realizar pentesting y revisión constante de vulnerabilidades.
- Realizar políticas de desarrollo seguro.
- Aseguramiento de equipos para el ingreso al sistema mediante Mac Address.
- Aseguramiento a los dispositivos móviles a través de mecanismos MDM (Mobile Device Management)
- Mantener los dispositivos móviles actualizados a la última versión para que permita ejecutar el software de aplicación segura.
- Aseguramiento del host del administrador implementando sistemas de endpoint management que estará constantemente en función de revisar las actualizaciones del sistema y vigilancia del antivirus.

5.3.3. Análisis sobre la capa de Red

Hallazgos

- No existe un control de ingreso.
- No existen mecanismos de autenticación, esto pone en riesgo la integridad y disponibilidad de la información de la base de datos.
- No existe una política de desarrollo seguro

Riesgos identificados

- Ingreso a la red sin autorización.
- Ataques a las bases de datos.
- Suplantación.

Recomendaciones

- Implementación de IPSs
- Restringir el ingreso de trafico por los puertos del servidor para evitar las denegaciones de servicios DDos

5.3.4. Análisis sobre la capa de datos

Hallazgos

- No existe seguridad entre la comunicación de la base de datos y el servidor
- No existe un aseguramiento entre la comunicación entre los dos servidores, principal y alterno.

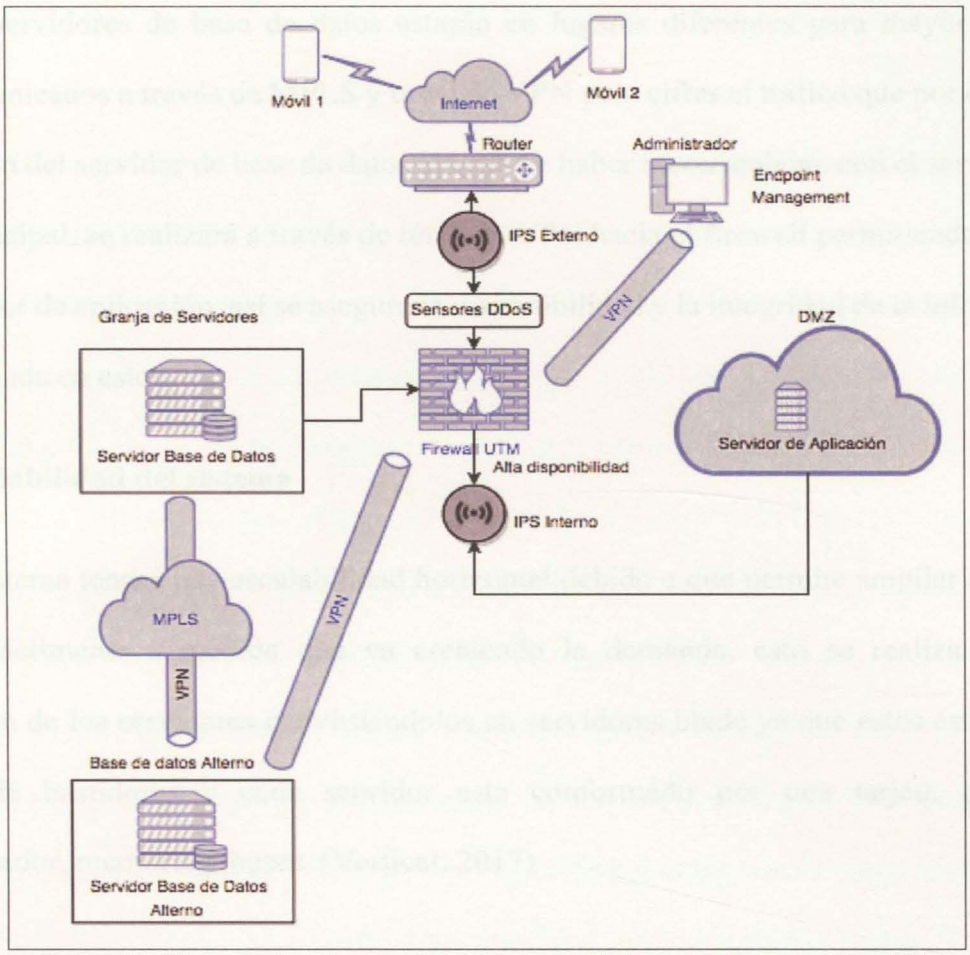
Riesgos identificados

- Ingreso a la red sin autorización.
- Comprometimiento de la información

Recomendaciones

- Separar la base de datos de los servidores evitando comprometer la información.
- Creación de granjas de servidores.
- Crear sistemas de transporte de comunicación segura de la información que pasa entre los dos servidores de base de datos.

El análisis de defensa en profundidad arrojo una serie de recomendaciones que permitieron dar una arquitectura de red mas robusta y mas segura como se muestra en la imagen 23, fortaleciendo la integridad y la disponibilidad de la información que reposa en las bases de datos y evitando los posibles ataques a la infraestructura planteada. (SANS Institute Information Security Reading Room, 2019)



Imágen 23. Diagrama de red asegurado y las recomendaciones arrojadas por el análisis

El PC de administrador se validará por medio de IP hacia el servidor de aplicación validándose por los protocolos programados en la IPS y firewall.

Para dar una mejor seguridad a los ataques de denegación de servicio DDoS, se programarán los puertos de los servidores que permitan el ingreso por este de un número determinados de peticiones.

El acceso a la base de datos se realizará mediante el ingreso al servidor de aplicación ubicado en la zona desmilitarizada (DMZ), en caso de que esta sea vulnerada la información no sufrirá ningún tipo de amenaza ya que todo el trafico debe pasar a través del IPS interno y el firewall UTM validando los parámetros de validación ingresados al firewall y al IPS interno.

Los servidores de base de datos estarán en lugares diferentes para mayor seguridad y estarán comunicados a través de MPLS y túnel de VPN para cifrar el trafico que por este pasa y la comunicación del servidor de base de datos alterno de haber inconveniente con el servidor de base de datos principal, se realizará a través de túnel de VPN hacia el firewall permitiendo la conexión con el servidor de aplicación, así se asegura la disponibilidad y la integridad de la información que está almacenada en estos.

5.4.Escalabilidad del sistema

El sistema tendrá una escalabilidad horizontal debido a que permite ampliar el número de servidores fácilmente a medida que va creciendo la demanda, esto se realiza mediante la virtualización de los servidores convirtiéndolos en servidores blade ya que estos están diseñados en forma de bastidores y cada servidor esta conformado por una tarjeta que contiene microprocesador, memoria y buses. (Vertical, 2017)

6. Conclusiones

La información presentada en esta investigación propone una alternativa a los modelos de plataformas tecnológicas de comunicaciones móviles que existen. Si bien, hay herramientas que permiten establecer comunicaciones móviles seguras en el mercado, éstas no cumplen con las especificaciones de seguridad de la información ya que el cifrado que emplea cada empresa que ofrece esta solución puede ser interceptada ya que ellos son los únicos que conocen el cifrado de dicha aplicación teniendo el conocimiento de las mismas, así mismo, las empresas tienen el control de los servidores donde está reposando la información que se recolecta en cada comunicación realizada, bien sea de texto, voz o multimedia. Por tal motivo y previendo lo anterior mente descrito se desarrolló un modelo de plataforma tecnológica de comunicación móvil celular que permita asegurar las comunicaciones estratégicas del Estado y así mitigar los riesgos que estos presenten a la hora de adquirir herramienta desarrollados por empresas de otros países.

En todas las comunicaciones móviles existen vulnerabilidades y éstas pueden ser explotadas mediante el uso de herramientas o técnicas de intrusión por parte de atacantes quienes pueden estar interesados en una comunicación específica que les permita recolectar información sensible o de interés para ellos, así como la exposición de la información del propio dispositivo, como es el IMEI e IMSI, exponiendo la integridad, disponibilidad o confidencialidad de la información de los usuarios. Por lo anterior, es importante poder identificar y contrarrestar las vulnerabilidades que se están presentando. Por tal motivo el modelo de comunicación móvil presentado tiene varias etapas de seguridad, como se explicó en el capítulo 4, donde cada interconexión de los datos que

viajan por el sistema está asegurada aminorando las vulnerabilidades que a lo largo de este trabajo de monografía se mencionan.

El análisis de las vulnerabilidades, que hacen posible que ocurra un incidente de seguridad y que se pueden presentar en las comunicaciones móviles como pueden ser malware, denegación de servicios, vulnerabilidades en la arquitectura de las redes móviles celular, son vulnerabilidades que los usuarios desconocen o no son conscientes de que se puedan presentar. Por lo anterior, la investigación realizada arrojó que es importante construir un modelo tecnológico de comunicación móvil celular segura, que permite contrarrestar incidentes de seguridad de la información que los usuarios están transmitiendo por ese medio y que corresponden a comunicaciones gubernamentales de alto valor.

Las comunicaciones convencionales empleadas mediante dispositivos móviles por parte de los miembros del alto gobierno, hacen que la información que se transmite a través de estos medios ponga en riesgo la integridad, disponibilidad o confidencialidad de esta, él modelo de comunicaciones seguras desarrollado en este trabajo, permitirá a los funcionarios de alto gobierno tener un canal seguro a través del cual puedan realizar las comunicaciones haciendo uso de dispositivos móviles celulares, evitando así los riesgos relacionados con la interceptación ilegal de comunicaciones, fuga de información, revelación de información con reserva legal y difusión de información a instituciones no pertinentes.

El modelo tecnológico descrito en esta investigación tiene varios aspectos importantes que se deben desarrollar y trabajar por separado para dar una adecuada funcionalidad a esta investigación,

como lo es el desarrollo del modelo del software, y el modelo de cifrado que posee este trabajo de monografía, vale aclarar que el desarrollo e implementación no se realiza en esta investigación, pero se propone a manera de sugerencia para futuros trabajos de grado.

7. Recomendaciones

Como líneas de acción a futuro, se recomienda que el modelo presentado sea desarrollado por una entidad idónea a esta tecnología como lo es el Ministerio de las comunicaciones, entidad que velará por el almacenamiento de la información que por esta plataforma se genere.

Una vez desarrollado el modelo este deberá tener unas capacitaciones para el uso y manejo de esta, como también la concientización en el uso que se le de al dispositivo y al empleo de la aplicación.

Para el desarrollo de la aplicación es importante tener un personal dedicado a cambiar cada semana el código de cifrado para minimizar el riesgo de interceptación de la comunicación y así fortalecer la seguridad de la plataforma.

8. Referencias

Díaz, C. A. (04 de 03 de 2011). *Enter.co*. Obtenido de CASI EL 75% DE LA POBLACIÓN MUNDIAL TIENE UN TELÉFONO MÓVIL: http://www.enter.co/cultura-digital/negocios/casi-el-75-de-la-poblacion-mundial-tiene-un-telefono-movil/

González, J. I. (Octubre de 2013). La importancia del teléfono móvil para la comunicación publicitaria. *Historia y Comunicación Social, 18*(Especial), 2.

Santiago, M. (24 de 05 de 2012). *Red Historia*. Obtenido de La invención del Telégrafo: https://redhistoria.com/la-invencion-del-telegrafo/

Aguilar, F. V. (2007). *Telefonos móviles : La nueva ventana para la comunicación integral.* Madrid: Creaciones Copyright S.L.

Boni, F. (2008). *Teoría de los medios de comunicación.* Valencia: Universitat de Valencia. Servei de Publicacions.

Couch, L. W. (2008). *Sistemas de comunicacioón digitales y análogos* . Monterrey, Ciudad Estado de Mejico, Mejico: Pearson.

Briceño, J. E. (2005). *Transmisión de datos.* Merida, Venezuela: Universidad de los Andes Ingeniería.

Jose Manuel Huidobro Moya, R. C. (2006). *Sistemas de Telefonía.* Madrid, España: Thomson Editor.

Judicatura, C. S. (1991). *Constitucoión Política de Colombia.* Bogotá.

Espectro, R. (1 de Mayo de 2017). *Mintic.* Obtenido de Sistema de Gestión del Espectro: http://www.mintic.gov.co/portal/604/w3-article-2350.html

John R. Pierce, A. M. (2002). *Señales: La Ciencia de las Telecomunicaciones.* New York, USA: Reverté S.A.

Tomasi, W. (2003). *Sistemas de Comunicaciones Electrónicas.* México: Prentice Hall.

Bedoya, J. (29 de Agosto de 2012). *Normatividad de las Telecomunicaciones*. Obtenido de http://juaco587.blogspot.com: http://juaco587.blogspot.com/2012/08/atribucion-de-bandas-de-frecuencia-del.html

Palma, J. D. (8 de Enero de 2018). Los detalles de Andrómeda, según la Procuraduría. *El Espectador*, págs. 1-7.

Joskowicz, J. (agosto de 2015). *iie.fing.edu.uy*. Obtenido de Conceptos Básicos de Telefonía: https://iie.fing.edu.uy/ense/asign/ccu/material/docs/Conceptos%20Basicos%20de%20Telefonia.pdf

Alison. (10 de septiembre de 2011). *tecnologiadelatelefoniacelular.blogspot.com*. Obtenido de Tecnología de la Telefonía Celular: http://tecnologiadelatelefoniacelular.blogspot.com/2011/08/la-telefonia-movil.html

Francisco Barceló, J. J. (2002). *Telefonía móvil: Caracterización de las conexiones.* Madrid: RA-MA S.A. Editorial y Publicaciones.

Jose Pico García, D. P. (2014). *Hacking y seguridad en comunicaciones Móviles GSM/GPRS/ UMTS y* . Madríd: 0xwOrd.

Mobile High Security. (2012). *CELLCRYPT*. Obtenido de mobilehighsec: http://www.mobilehighsec.com/b5e3ff41-50b2/soluciones.html

Simonite, T. (20 de 3 de 2014). *Un 'smartphone' a prueba de la NSA por 3.500 dólares*. Obtenido de MIT technology review: https://www.technologyreview.es/s/4115/un-smartphone-prueba-de-la-nsa-por-3500-dolares

METZ, C. (04 de 05 de 2016). *WIRED*. Obtenido de FORGET APPLE VS. THE FBI: WHATSAPP JUST SWITCHED ON ENCRYPTION FOR A BILLION PEOPLE:

https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/#slide-7

Diario Información. (02 de 02 de 2018). *Tecnología*. Obtenido de Signal, así es la 'app' que recomienda Snowden y usan Puigdemont y Comín: https://www.diarioinformacion.com/vida-y-estilo/tecnologia/2018/01/31/signal-app-recomendada-snowden-puigdemont/1983528.html

247 Tecno. (24 de 12 de 2017). *247 Tecno*. Obtenido de Telegram: http://247tecno.com/telegram/

Kalenderi, M., Pnevmatikatos, D., Ioannis, P., & Charalampos, M. (29 de 08 de 2012). BREAKING THE GSM A5/1 CRYPTOGRAPHY ALGORITHM WITH RAINBOW TABLES AND HIGH-END FPGAS . Oslo, Noruega.

José Pico, D. P. (2014). *Hacking y Seguridad en Comunicaciones Móviles GSM/GPRS/UMTS/LTE.* MADRID: OXWORD.

Fernandez, Y. C., & Rizo, F. M. (Mayo de 2014). LTE vs. WiMAX. *Revisra Telemática, 13*(2), 42-52.

Muñoz, J. G. (Septiembre de 2016). Estudio de la arquitectura de protocolos de LTE. Barcelona.

Griffa, E. (2007). ¿Por qué "all IP"? *Gerencia*.

Dejun Yang, G. X. (2013). Coping with a Smart Jammer in Wireless Networks. *IEEE*, 4038-4045.

Monowar Hasan, E. H. (2013). Random access for machine-to-machine communication in LTE-advanced networks. *EEE Communications Society*.

Bartolomé, L. (26 de Febrero de 2018). *ElEconomista.es*. Obtenido de El Economista: http://www.eleconomista.es/tecnologia/noticias/8963826/02/18/Android-el-sistema-operativo-preferido-por-los-ciberdelincuentes.html

Luque, S. (28 de Marzo de 2017). *Xataka*. Obtenido de Xataka.com: https://www.xatakandroid.com/seguridad/los-ataques-de-malware-en-dispositivos-moviles-aumentan-y-android-es-el-principal-objetivo-segun-nokia

Alonso C., G. P. (2013). *Hacking de dispositivos IOS: iPhone & iPad.* Madrid, Móstoles: 0xWord.

Owasp. (13 de Febrero de 2017). *Owasp*. Obtenido de Owasp.org: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Cao, J., M. M., & H. L. (2012). An uniform handover authentication between E-UTRAN and Non-3GPP access networks. *IEEE.org, 11*(10), 3644-3650.

Centro Criptologico Nacional. (2013). *Seguridad en dispositivos móviles.* Madrid: Gobierno de España, Ministerio de la Presidencia.

Germán Darío Arias Pimiento, G. B. (Agosto de 2016). *CÓDIGO DE BUENAS PRÁCTICAS PARA EL DESPLIEGUE DE REDES DE COMUNICACIONES*. Obtenido de Comisión de Regulación de Comunicaciones : https://www.crcom.gov.co/recursos_user/2016/Informes/Codigo_Buenas_Practicas_2016.pdf

Presidencia de la República. (2018). *presidencia* . Obtenido de Gobierno: https://id.presidencia.gov.co/gobierno/presidente-ivan-duque

UIT, U. T. (2004). Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo. Ginebra.

Torres, C. (19 de Abril de 2014). *ANDROIDSIS* . Obtenido de androidsis.com: https://www.androidsis.com/que-es-un-hard-reset-y-para-que-se-utiliza/

UIT-T. (Junio de 2006). La seguridad en las telecomunicaciones y las tecnologías de la información.

Larragan, M. G. (14 de Julio de 2016). *Criptología para todos*. Obtenido de manQiTgestión: http://mikelgarcialarragan.blogspot.com/2016/07/criptografia-xxi-criptologia-para-todos.html

Redacción Judicial El Espectador. (14 de Enero de 2019). A juicio general (r) Humberto Guatibonza por caso de chuzadas ilegales. *El Espectador*, págs. 1-6.

SANS Institute Information Security Reading Room. (2019). Defense In Depth.

Vertical, E. H. (7 de Marzo de 2017). *Oscar Blancarte Software Architect.* Obtenido de www.oscarblancarteblog.com: https://www.oscarblancarteblog.com/2017/03/07/escalabilidad-horizontal-y-vertical/

Anexos

PRUEBAS DE SIMULACIÓN DEL MODELO

A continuación, se describe el alcance del desarrollo de un sistema propietario de comunicación móvil segura entre dos dispositivos móviles que permitirá demostrar el modelo del trabajo de monografía titulado **"Diseño de un modelo de plataforma tecnológica que permita brindar seguridad a las comunicaciones estratégicas del Estado a través de dispositivos móvil celular"**.

El objetivo de esta simulación es demostrar que se puede efectuar una comunicación entre dos dispositivos móviles Android mediante una aplicación que se instalará a los 2 terminales. Así mismo el sistema tendrá un sencillo algoritmo de cifrado pudiendo demostrar el flujo de la comunicación entre los 2 terminales y un servidor a través de una misma red, como se puede apreciar en la Imagen 22.

Imagen 24. Esquema del modelo

- **Etapa de comunicación**

En esta etapa el dispositivo móvil 1 y el dispositivo móvil 2 se conectarán a través de un computador que hará las veces de servidor, sirviendo de enlace de tráfico y de seguridad.

- **Funcionamiento**
- El dispositivo móvil 1 solicita al servidor acceso a una comunicación segura hacia el dispositivo móvil 2
- El servidor verifica que el dispositivo móvil 2 esté disponible y le envía la solicitud a cada uno las llaves de seguridad que van a usar sobre el protocolo de encripción.
- El dispositivo móvil 1 usando las llaves del ítem de solicitud envía las tramas hacia el servidor.

  El servidor envía las tramas de datos hacia el dispositivo móvil 2.

- **Verificación.**
- Realizar pruebas de comunicación exitosa entre los dos dispositivos.
- El servidor enviará una llave de seguridad al dispositivo móvil 1 y otra al dispositivo móvil 2 para verificar la integridad de la información recibida.
- Verificar conexión. Se verificará en caso de que se desconecte el dispositivo móvil 2 y se pierda la comunicación.
- Realizar pruebas de transmisión sin utilizar protocolos de cifrado.

Condiciones de la prueba

- El canal físico de comunicación será un router WIFI.
- Las pruebas de transmisión se realizarán enviando caracteres tipo chat y de voz.

- Se aplicará un sencillo algoritmo de codificación de la comunicación, el cual permitirá modificar las llaves para realizar diferentes pruebas.

Las pruebas realizadas arrojaron que, si el sistema de cifrado que genera la aplicación es modificado, el sistema no descifra ningún tipo de comunicación tanto de voz como de texto, los dispositivos podrán escucharse de manera óptima siempre que el código de cifrado coincida en los dos dispositivos como se aprecia en la Imagen 23.

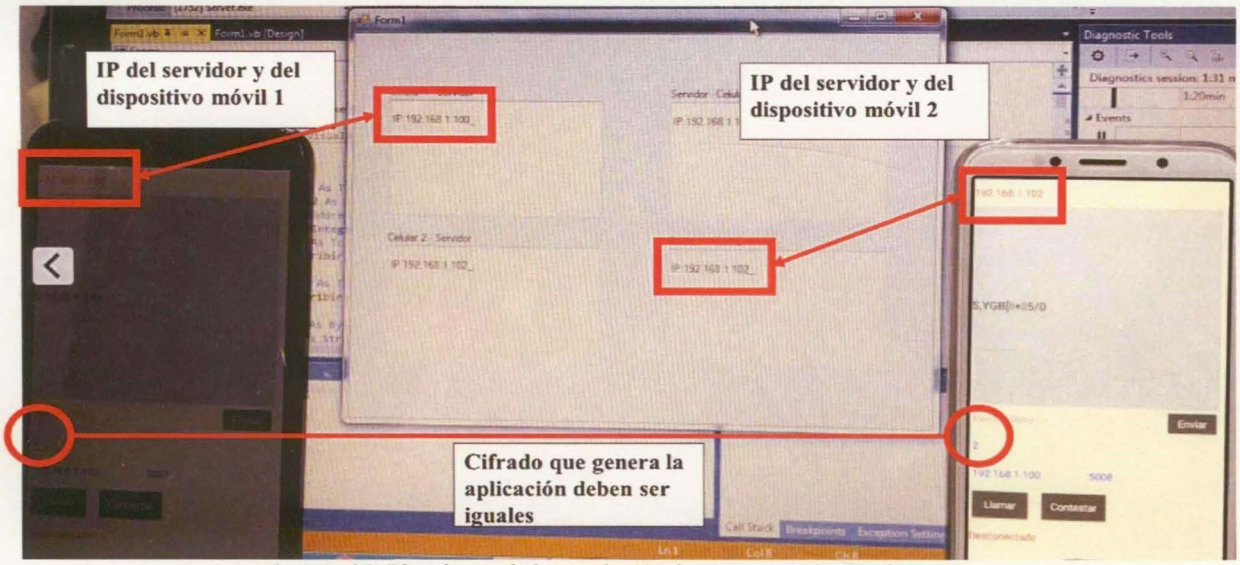


Imagen 25. Plataforma de la simulación de comunicación móvil segura.

Así mismo se anexa el código fuente de la APK módulo de audio, APK módulo de texto programado con el software para programar aplicaciones de Android "basic4android" y el código fuente del servidor programado en "visual Basic".