ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

TEMA: DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA PARA LA DETECCIÓN DE OTT *BYPASS* (VIBER) PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

AUTOR: CABRERA OCHOA, ANDRÉS FELIPE

DIRECTOR: ING. TORRES, JULIO

SANGOLQUÍ

2016

CERTIFICACIÓN

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que el trabajo de titulación, "**DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA PARA LA DETECCIÓN DE OTT BYPASS (VIBER) PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP**" realizado por el señor **ANDRÉS FELIPE CABRERA OCHOA**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor **ANDRÉS FELIPE CABRERA OCHOA** para que lo sustente públicamente.

Sangolquí, 19 de diciembre de 2016

Ing. Julio Wladimir Torres Tello.

DIRECTOR

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

AUTORÍA DE RESPONSABILIDAD

Yo, **ANDRÉS FELIPE CABRERA OCHOA**, con cédula de identidad Nº 1104690274 declaro que este trabajo de titulación **"DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA PARA LA DETECCIÓN DE OTT BYPASS (VIBER) PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP"** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 19 de diciembre de 2016

.....

ANDRÉS FELIPE CABRERA OCHOA

C.C.: 1104690274

AUTORIZACIÓN

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **ANDRÉS FELIPE CABRERA OCHOA**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA PARA LA DETECCIÓN DE OTT BYPASS (VIBER) PARA LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 19 de diciembre de 2016

ANDRÉS FELIPE CABRERA OCHOA

C.C.: 1104690274

DEDICATORIA

El presente trabajo de investigación está dedicado a mi Abuelita Fabiola (+), a mis padres Ney y Sandra, y a mi familia que gracias a ellos he logrado el cumplimiento de este y otros proyectos que a lo largo de mi vida me los he planteado y a mi hermana Paula por ser parte fundamental en mi vida.

Andrés Felipe Cabrera Ochoa

AGRADECIMIENTO

Agradezco a Dios por permitirme llegar a cumplir esta meta y a pesar de todo no dejar de protegerme a cada instante.

A mis padres por haberme impulsado y apoyado para tomar decisiones que me han llevado a llegar a culminar esta etapa y por haberme apoyado en todo momento haciendo que nunca me faltara nada. A mi hermana por ser parte vital de mi vida convirtiéndose en mi amiga y mi confidente.

A mi familia que siempre han estado pendiente de mi a lo largo de mi vida, aconsejándome y ayudándome en todo momento.

Agradezco a mi Director de tesis, Ing. Julio Torres, principalmente por darme la oportunidad de trabajar en un proyecto de gran importancia, por guiarme con sus conocimientos para la culminación de esta etapa de mi vida y al Ing. Luis Estévez, por darme la oportunidad de desarrollar mi trabajo de investigación en la Jefatura de Prevención de Fraude de la CNT EP.

A mis amigos, que gracias a su apoyo y ayuda han sido parte vital para la culminación de una meta más en mi vida.

Andrés Felipe Cabrera Ochoa

ÍNDICE GENERAL

CERTIFICADO **ii**

DECLARACIÓN DE RESPONSABILIDAD **iii**

AUTORIZACIÓN **iv**

DEDICATORIA **v**

AGRADECIMIENTO **vi**

ÍNDICE GENERAL **vii**

ÍNDICE DE TABLAS **xi**

ÍNDICE DE FIGURAS **xiii**

RESUMEN **xv**

ABSTRACT **xvi**

1 INTRODUCCIÓN **1**

1.1 Antecedentes 1

1.2 Justificación e Importancia 2

1.3 Alcance del Proyecto 4

1.4 Objetivos 5

1.4.1 General 5

1.4.2 Específicos 5

2 MARCO CONCEPTUAL **7**

2.1 OTT (*Over The Top*) 7

2.2 Viber 8

2.3 Android 9

2.3.1 Principales versiones del sistema operativo Android 10

2.3.2 Android Studio 12

2.4 VoIP (*Voice Over Internet Protocol*) 13

2.4.1 Ventajas de VoIP 13

2.5 Fraude 14

2.5.1 Definición de Fraude 14

2.5.2 Fraude en Telecomunicaciones: 14

2.5.3 Control de Fraude 15

2.6 Fraude ByPass 16

2.7 OTT Bypass 18

2.8 Métodos de control para Fraude en Telecomunicaciones 19

2.8.1 Pruebas de lazo (loop) 19

2.8.2 Escenario actual de pruebas para detección de fraude de la CNT EP 20

2.9 Sotfware 21

2.9.1 Base de Datos 21

2.9.2 MySQL 23

2.9.3 Lenguaje PHP 24

3 DISEÑO Y DESARROLLO **26**

3.1 Estructura del sistema. 26

3.1.1 Requerimientos 28

3.1.2 Herramientas y recursos 31

3.2 Desarrollo de la aplicación móvil para la generación de llamadas. . . . 31

3.2.1 Modos de funcionamiento de la Aplicación Móvil 32
3.2.2 Interfaz de usuario del aplicativo móvil. 35
3.3 Comunicación con el servidor. 40
3.3.1 Clase AppConfig 40
3.3.2 Clase AppController 40
3.4 Almacenamiento temporal de los elementos 40
3.4.1 Clase Session Manager 41
3.4.2 Clase SQLiteHandler 41
3.5 Selección del modo de funcionamiento 41
3.5.1 Clase MainActivity 42
3.6 Almacenar Tarjetas 42
3.6.1 Clase Register 42
3.7 Ejecución del Loop 43
3.7.1 Clase leerdatos 43
3.8 Implementación del Servidor 44
3.8.1 Diseño de la base de datos 44
3.8.2 Servidor Web para la aplicación 45

4 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA 48
4.1 Funcionamiento de la aplicación móvil. 48
4.2 Funcionamiento de la aplicación Web. 49
4.3 Protocolos de Prueba 50
4.3.1 Registro de Tarjetas. 50
4.3.2 Generador de Loop de llamadas. 51
4.4 Análisis de Resultados 60
4.4.1 Pruebas a través de conexión SMA 61
4.4.2 Pruebas de conexión WiFi 61
4.4.3 Variación de Operadora 62
4.4.4 Resumen de resultados 62

5 CONCLUSIONES Y RECOMENDACIONES **64**

5.1 Conclusiones 64

5.2 Recomendaciones 67

BIBLIOGRAFÍA **70**

ÍNDICE DE TABLAS

1 Parámetros Requeridos. 29
2 Parámetros Requeridos. 30
3 Componentes ventana principal. 36
4 Componentes ventana almacenar. 38
5 Componentes Ventana Ejecución. 39
6 Valores de parámetros de conexión. 46
7 Pruebas de Funcionamiento de la Aplicación Móvil. 49
8 Pruebas de Funcionamiento de la Aplicación Web. 50
9 Tarjetas Ingresadas. 51
10 Llamadas 2G. 52
11 Llamadas Completadas 2G. 53
12 Llamadas 3G o H+. 53
13 Llamadas Completadas 3G o H+.-. 54
14 Llamadas 4G. 54
15 Llamadas Completadas 4G. 55
16 Llamadas Movistar. 55
17 Llamadas Completadas Movistar. 56
18 Llamadas Claro. 56
19 Llamadas Completadas Claro. 57
20 Llamadas CNT. 57
21 Llamadas Completadas CNT. 58

22 Llamadas Tv Cable. 58
23 Llamadas Completadas Tv Cable. 59
24 Llamadas Netlife. 59
25 Llamadas Completadas NetLife. 60
26 Cuadro Pruebas CNT. 63
27 Cuadro Pruebas Otros Escenarios. 63

ÍNDICE DE FIGURAS

1 Diagrama del Sistema de Detección de OTT Bypass. 5

2 Aplicativos OTT. **Fuente:**Singarayar (2016) 8

3 Aplicativo OTT Viber. **Fuente:**Viber (2016a) 8

4 Distribución Android. **Fuente:**Android (2016a) 10

5 Android Studio. 12

6 Diagrama Proceso de control de fraude. 15

7 Definición ByPass. 16

8 Ruta legal ingreso de llamada internacional. 17

9 Ruta ilegal ingreso de llamada internacional. 17

10 Diagrama OTT Bypass. 18

11 Diagrama pruebas de lazo. **Fuente:** Orquera (2014) 20

12 Diagrama Cliente-Servidor. 27

13 Diagrama de bloques del sistema. 32

14 Diagrama UML casos de uso. 33

15 Diagrama UML de Clases 34

16 Ventana Principal. 36

17 Ventana Almacenar. 37

18 Ventana Llamar. 39

19 Ventana Principal. 41

20 Variación de Conexión. 61

21 Variación de conexión Wifi. 61
22 Variación de Operadora. 62

RESUMEN

El presente proyecto describe el diseño e implementación de un sistema para la detección de Fraude OTT (*Over the Top*) efectuado a través OTT Viber, consta de una aplicación móvil desarrollada y funcionando sobre la plataforma Android y el desarrollo de un servidor WEB implementado enteramente en lenguaje PHP. El sistema cuantifica la cantidad de tráfico de llamadas internacionales entrantes en la red de la Corporación Nacional de Telecomunicaciones CNT EP y el tráfico entrante por medio del OTT Viber, permitiendo analizar esta información y presentar un informe detallado por medio del servidor Web. Para el desarrollo se utilizó dos terminales móviles con sistema operativo Android (Alcatel Idol 3 y Samsung Galaxy J1 ACE). En el diseño se estableció por parte de la Corporación Nacional de Telecomunicaciones CNT EP los requerimientos y parámetros que debía cumplir tanto el generador como receptor de llamadas y en base a estos parámetros se implementó una base de datos con la finalidad de obtener y almacenar todos los datos necesarios para el correcto funcionamiento del sistema. Conforme a los parámetros se desarrolló el software necesario para cumplir con todos los requerimientos en la plataforma Android Studio. Los resultados de las pruebas realizadas al culminar el desarrollo de este proyecto de investigación demostraron que el sistema cumplió con todos los objetivos propuestos, además el software es compatible con todos los dispositivos móviles con sistema operativo Android a partir de la versión 4.1.

PALABRAS CLAVE:

- *OTT BYPASS*
- ANDROID
- VIBER
- PHP
- FRAUDE

ABSTRACT

The present project describes the design and implementation of a system for the detection of OTT (Over The Top) Fraud through OTT Viber, consists of a mobile application developed and running on the Android platform and the development of a WEB server implemented entirely in PHP language. The system quantifies the amount of incoming international call traffic in the National Telecommunications Corporation CNT EP network and incoming traffic through OTT Viber, allowing the analysis of this information and a detailed report through the Web server. For development, two mobile terminals were used with Android operating system (Alcatel Idol 3 and Samsung Galaxy J1 ACE). The design established by the National Telecommunications Corporation CNT EP the requirements and parameters to be met by both the generator and receiver of calls and based on these parameters a database was implemented in order to obtain and store all the data necessary for the correct operation of the system. According to the parameters, the necessary software was developed to meet all the requirements in the Android Studio platform. The results of the tests carried out at the end of the development of this research project showed that the system fulfilled all the proposed objectives, besides the software Is compatible with all mobile devices with Android operating system as of version 4.1.

KEY WORDS:

- *OTT BYPASS*
- ANDROID
- VIBER
- PHP
- FRAUD

CAPÍTULO 1

INTRODUCCIÓN

1.1 Antecedentes

Los fraudes en el área de las telecomunicaciones móviles se han detectado en el Ecuador desde aproximadamente 1995 con el fraude denominado "*Call Back*", convirtiéndose este en el primer tipo de fraude identificado en nuestro país (Orquera, 2014).

En 1996 se detecta el segundo tipo de fraude en telecomunicaciones, el cual se efectúa a través de los denominados Sistemas de *Bypass*. Para este entonces, estos novedosos sistemas se implementaban únicamente con el uso de líneas fijas, a través de las cuales, se terminaba de cursar las llamadas telefónicas de origen internacional como si fueran llamadas locales. Cuando se lo descubrió, este sistema fue sancionado administrativamente por la Superintendencia de Telecomunicaciones, SUPERTEL, conforme el marco legal vigente en 1996. A partir del 12 de agosto de 1999 los Sistemas de *Bypass* se pudieron combatir frontalmente mediante la aplicación del Artículo 422 del Código Penal reformado en dicha fecha por el H. Congreso Nacional por iniciativa de la SUPERTEL (Orquera, 2014).

En el año 2003, aparecen por primera vez en el Ecuador la implementación de Sistemas *Bypass* con líneas celulares, hecho que puso en marcha una nueva etapa dentro del combate a los fraudes en telecomunicaciones en el Ecuador, ya que estos sistemas

al contar con infraestructura física reducida se volvieron más difíciles de ubicar y controlar (Meza, 2007).

En el 2014 entró en vigencia el Nuevo Código Integral Penal, el mismo que introdujo nuevas regulaciones en cuanto a fraude en las Telecomunicaciones, en donde se estipulan las sanciones a personas o empresas que proporcionen el servicio de telecomunicaciones de una forma ilegal o que perjudique a las operadoras o prestadoras de este servicio.

Para el año 2015 se identificó en Ecuador una nueva forma de fraude en telecomunicaciones conocida como OTT (*Over The Top*) *Bypass* (F. Castillo, 2015) , el cual está empezando a causar grandes pérdidas económicas a los operadores, ya que normalmente la conexión de una llamada de voz da lugar al pago de una tarifa de terminación (el precio pagado por el operador generador de la llamada al operador receptor de la llamada por la terminación de una llamada en su red). El incremento de las ventas de teléfonos inteligentes y el uso de servicios OTT pone en riesgo una parte cada vez mayor de los ingresos por terminación: cuando un usuario móvil envía un mensaje de Whatsapp (en lugar de un SMS), o cuando efectúa una llamada "Viber a Viber" (en lugar de una llamada de voz internacional), sencillamente no hay tarifa de terminación (Arraxe, s.f). Por esta razón es necesario encontrar un método eficiente de prevención, detección y control, haciendo que los aplicativos se limiten a prestar los servicios que ofrecen dentro de sus mismos usuarios y no así ofrecer servicios que no se encuentran dentro de la competencia del aplicativo y por los cuales no paga ningún tributo, teniendo dentro de estos servicios la terminación de llamadas internacionales originadas desde un medio normal y no desde un aplicativo OTT.

1.2 Justificación e Importancia

La telefonía móvil ha avanzado de manera agigantada en los últimos años y ha generado varias plazas de trabajo en las operadoras de este servicio, es por esto que se

debe evitar cualquier tipo de fraude o desfalco para asegurar la rentabilidad de las compañías y en consecuencia la permanencia y crecimiento de las operadoras en óptimas condiciones.

En un mercado económicamente relevante como es el de las telecomunicaciones, que representan el 3,46% de PIB del Ecuador, donde en 2006 la telefonía móvil tenía una penetración de 63,2%, y hoy se encuentra con penetración del 104,89% lo que se traduce en 16´854.515 de líneas activas (de Telecomunicaciones y Sociedad de la Información, 2016), "la ARCOTEL investigó alrededor de 13 casos sobre la prestación no autorizada del servicio telefónico de larga distancia internacional, los cuales fueron presentados ante la Fiscalía, a través de ocho denuncias, que abarcan un total de 2.926 números telefónicos detectados conforme a los métodos y procedimientos técnicos establecidos" (de Telecomunicaciones y Sociedad de la Información, 2016), dando así como evidencia que el fraude causa un impacto importante en el sector.

En el 2007 la SUPERTEL expuso que según diferentes fuentes calculan que las compañías pierden cerca del 10% de sus ingresos por falta de herramientas tecnológicas y de procedimientos para la detección y el control del fraude y aseguramiento de ingresos, que con los márgenes de ganancia comprometen la supervivencia de las compañías (Meza, 2007).

La Corporación Nacional de Telecomunicaciones EP se ve directamente afectada al ser una empresa proveedora del servicio de telefonía móvil y de larga distancia internacional, por lo tanto el desarrollo e implementación de un sistema de detección de eventos de OTT Bypass permitirá crear métodos de prevención y control de este tipo de fraude.

1.3 Alcance del Proyecto

El proyecto pretende realizar un análisis de la pérdida de tráfico de Larga Distancia Internacional (LDI) entrante mediante *Bypass* por OTT (Viber), entregando como producto final un sistema que permita la detección de un posible OTT Bypass efectuado por medio de la aplicación Viber. Los aplicativos desarrollados deberán ser instalados en teléfonos inteligentes con sistema operativo Android, el mismo que servirá para generar, detectar y analizar la ruta de ingreso de las llamadas internacionales entrantes. El sistema podrá discriminar cuando la llamada termina por la aplicación Viber y cuando termina en la red pública conmutada de la Corporación Nacional de Telecomunicaciones CNT EP (escenario sin OTT *Bypass*).

Las pruebas se desarrollarán bajo dos escenarios: el primero corresponderá a una conexión del equipo con todas las redes móviles de CNT, es decir, en 2G, 3G o 4G, adicionalmente se realizarán pruebas con la red 4G de los operadores Claro y Movistar. Mientras que el segundo escenario se efectuará cuando el terminal se encuentre conectado a una red WiFi.

El sistema constará de dos teléfonos inteligentes, uno que funcionará como un sistema de generación de llamadas de lazo y otro que funcionará como receptor de las llamadas generadas por el primer teléfono, este último se encontrará en conexión con un ordenador o PC para el procesamiento de la información y la presentación de informes detallados de los eventos generados en las pruebas.

Como se puede obervar en el diagrama expuesto en la figura 1, se implementará además un servidor WEB, en el cuál se diseñará y creará una base de datos para almacenar la información provista por los teléfonos inteligentes que se encontrarán funcionando como generador y receptor de las llamadas de lazo. Dicha información contendrá datos importantes como la ruta por la cual ingresó la llamada, fecha, hora y el número de origen. Se implementará además una aplicación WEB mediante la cual se podrá realizar la monitorización remota de la información desde un ordenador au-

torizado, todo esto mediante una interfaz que permitirá la conexión de los diferentes aplicativos desarrollados. La seguridad de las redes y sistemas es responsabilidad de CNT EP.

Figura 1: Diagrama del Sistema de Detección de OTT Bypass.

1.4 Objetivos

1.4.1 General

- Desarrollo de una herramienta para análisis de pérdida de tráfico de Larga Distancia Internacional (LDI) entrante mediante *Bypass* por OTT (Viber).

1.4.2 Específicos

- Realizar un estudio acerca del escenario actual de pruebas para la detección de fraude telefónico de la Corporación Nacional de Telecomunicaciones CNT EP.
- Analizar las propiedades y capacidades del sistema operativo Android a partir de la versión 2.3, en el ámbito de la comunicación celular y la ejecución de las aplicaciones OTT, junto con su entorno de desarrollo de aplicaciones.
- Analizar la funcionalidad y prestaciones de la aplicación para comunicación móvil Viber.

- Investigar la ocurrencia e intensidad del OTT *Bypass* por medio de Viber en la CNT EP.
- Desarrollar una aplicación para dispositivos móviles que permita generar llamadas de lazo hacia otro dispositivo móvil de forma consecutiva y que permita configurar los parámetros requeridos para completar dichas llamadas.
- Desarrollar una aplicación para dispositivos móviles Android en la cual permita detectar un posible OTT *Bypass*, por medio de la aplicación Viber, mediante el análisis de la información proporcionada de las llamadas entrantes.
- Desarrollar una aplicación en el servidor para la monitorización remota del sistema de detección de OTT *Bypass*.
- Evaluar el desempeño del sistema de detección de OTT *Bypass*, por medio de simulaciones y llamadas forzadas.

CAPÍTULO 2

MARCO CONCEPTUAL

En esta sección se realizará una revisión de los conceptos principales de los recursos y tecnologías utilizadas a lo largo de todo el desarrollo e implementación de este proyecto de investigación, partiendo desde los conceptos y utilidades del software utilizado, hasta los distintos lenguajes y herramientas de programación.

2.1 OTT (*Over The Top*)

Las aplicaciones OTT como Skype, Viber, Whatsapp, GO ver figura 2, son aplicaciones que ofrecen una alternativa de bajo costo a servicios móviles como lo es voz y mensajería (SMS) tradicional, incluyen también servicios de comunicación adicionales como lo son llamadas de video, grupos de chat y las comunicaciones basadas en texto (s.n, 2014). Todo esto por medio de uso de la red de internet, es decir servicios comunicación sobre IP.

Figura 2: Aplicativos OTT.

Fuente: Singarayar (2016)

2.2 Viber

Figura 3: Aplicativo OTT Viber.

Fuente: Viber (2016a)

Este aplicativo brinda el servicio gratuito de envio de mensajes y realización de llamadas desde un teléfono inteligente a cualquier dispositivo que tenga instalado Viber y cuente con conexión a Internet. Viber se encuentra integrado con el sistema operativo Android para otorgarle la mejor experiencia y rendimiento. Al instalar Viber por primera vez en un teléfono inteligente este aplicativo se sincroniza con sus contactos y detecta cuáles ya son usuarios Viber, permitiendo así seleccionar un contacto y hablar o mensajear gratis (Viber, 2016b).

Dentro de las características principales se tiene(Viber, 2016b):

- Texto libre, mensajes con fotos y vídeo con ubicaciones compartidas
- Llamadas VoIP de la mejor calidad utilizando 3G, 4G o WiFi.
- Viber Out es una herramienta que permite hacer llamadas a números móviles o fijos incluso no siendo de usuarios del aplicativo Viber.
- Es compatible con tabletas Android, dando así la facilidad de usar un teléfono inteligente o una tableta al mismo tiempo.
- Servicio de mensajería grupal hasta con 100 usuarios Viber.

Al ser una de las pocas OTT que ofrecen calidad de servicio en sus llamadas y ofrecer terminación de llamadas por medio de Viber Out, se presta para que también realice la terminación de llamadas internacionales, basta solo con el que el usuario receptor de la llamada tenga instalado el aplicativo en su teléfono y que tenga una conexión a Internet con buen ancho de banda (Viber, 2016b).

Al poseer la característica de calidad de servicio y tomando en cuenta los resultados que se presentaran en el capítulo 4 podemos suponer que esto implica una vulnerabilidad para los operadores nacionales que brindan servicio de voz y datos, puesto que esto podría favorecer el aparecimiento de fraude OTT.

2.3 Android

Android es un conjunto de software de código abierto que se creó para una amplia gama de dispositivos móviles, que se originó por un grupo de empresas llamado *Open Handset Alliance*, encabezada por Google (Android, 2015).

La principal característica que le ha dado a Android su éxito y popularidad es ser una plataforma de software libre, permitiendo así que los usuarios y desarrolladores potencien y maximicen el aprovechamiento de las capacidades del dispositivo móvil.

Además, presenta un acoplamiento único con distintos dispositivos ya que al ser software multiplataforma se adapta fácilmente a las distintas características o factores de forma como el tamaño de pantalla.

2.3.1 Principales versiones del sistema operativo Android

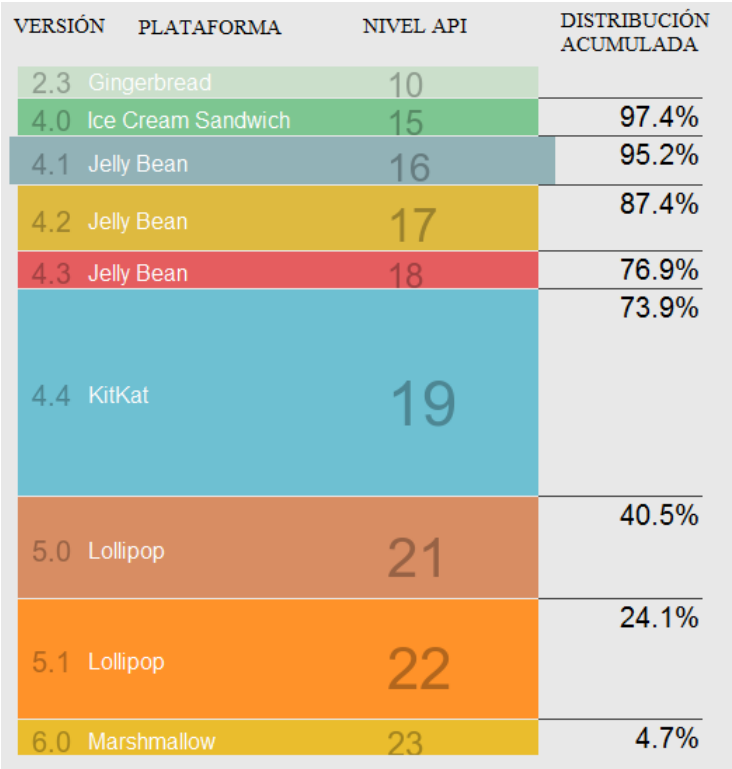


Figura 4: Distribución Android.

Fuente: Android (2016a)

2.3.1.1 Android 2.3 *Gingerbread*

Es una de las primeras versiones que tienen como característica una interfaz más rápida y efectiva en cuanto al consumo de batería, consta con un nuevo teclado con función de sugerencia al momento de escribir, mejora notablemente en consumo de batería, ya que cierra aplicaciones que se encuentren en segundo plano y no se encuentren usándose.Esta es la primera versión en donde se implementan las llamadas VoIP y compatibilidad con comunicaciones de campo cercano (NFC) (TICbeat, 2010).

En cuanto a desarrollo se ha implementado una máquina virtual denominada *Dalvik*, que funciona como recolector de basura minimizando así las pausas que se pueden presentar en la aplicación, los eventos táctiles son tratados de una forma mas eficiente y rápida haciendo que la utilización del CPU disminuya notablemente (R. TICbeat, 2010).

2.3.1.2 Android 4.0 *ICE CREAM SANDWICH*

Actualmente es la versión mas popular, debido que alcanza un uso de 97.4% en los dispositivos móviles con sistema operativo Android Android (2016b). Incluye mejoras como el reconocimiento facial y de voz, compatibilidad absoluta con tecnología NFC, optimización en cuanto al navegador del sistema de carpetas(Gonzáles, 2012).

Se integra un sistema de control de gastos o consumo de datos, indicando el consumo global por fecha, e incluso permitiendo poner un límite de consumo y cuando este límite esté pronto a superarse se enviará una alerta. Para navegación tiene una sincronización con Google Chrome en modo escritorio, permitiendo con una sola cuenta tener el historial de navegación y preferencias tanto en un PC como en un teléfono móvil(Raya, 2011).

2.3.1.3 Android 4.1 *Jelly Bean*

Jelly Bean es una versión del sistema operativo Android optimizado para ofrecer un rendimiento mejorado y una menor latencia en el proceso táctil en comparación a sus versiones anteriores, además presenta una interfaz intuitiva haciendo su manejo mucho más fácil al usuario. Es una versión muy completa ya que está diseñado para trabajar con la herramienta *systrace*, la misma que permite que los datos sean recogidos directamente desde el núcleo de Linux para presentar así una imagen global de todas las actividades que se encuentra ejecutando el sistema (Developer, 2016).

Si bien la versión 4.1 no es la versión más actualizada de esta plataforma, se la escogió puesto que es la más completa de las más antiguas teniendo las funcionali-

dades requeridas para un óptimo desempeño de un teléfono inteligente y viene instalada desde fábrica en los teléfonos inteligentes a usar como generador y receptor de llamadas, permitiendo así aumentar la compatibilidad del aplicativo con los distintos modelos y variedades de dispositivos móviles que cuentan con este sistema.

2.3.2 Android Studio

Figura 5: Android Studio.

Android Studio es un entorno de desarrollo integrado que brinda un sinnúmero de herramientas para el desarrollo y la implementación de cualquier aplicación para todos los dispositivos Android, permitiendo realizar la edición de código de primer nivel.

Dentro de las funciones que ofrece Android Studio tenemos(Android, 2016b):

- Sistema de compilación flexible basado en *Gradle*, el cual básicamente es una herramienta que permite automatizar el proceso de construcción de un proyecto teniendo a cargo como funciones compilar, pruebas y empaquetado
- Emulador rápido con varias funciones.
- Un entorno unificado en el que se puede realizar desarrollos para todos los dispositivos Android.

- *Instant Run*, para realizar cambios mientras la app se encuentra ejecutandose sin la necesidad de compilar un nuevo APK (*Android Application Package*).
- Integración de plantillas de código y *GitHub* que es una plataforma colaborativa para ayudar a compilar funciones comunes de las apps e importar ejemplos de código.
- Gran cantidad y variedad de herramientas y *frameworks* de prueba.
- Herramientas *Lint* para detección de problemas de rendimiento, uso, compatibilidad de versión, etc.
- Compatible con C++ y NDK (*Native Development Kit*).
- "Soporte integrado para *Google Cloud Platform*, que facilita la integración de *Google Cloud Messaging* y *App Engine*", lo cual permite trabajar en un proyecto desde cualquier parte del mundo accediendo con un correo personal y cuenta de estas plataformas.

2.4 VoIP (*Voice Over Internet Protocol*)

VoIP es una tecnología utilizada para la transmisión de voz sobre una red de datos como lo es el Internet usando para este propósito el protocolo IP. La VoIP digitaliza las señales de voz y las convierte en paquetes de datos comprimidos que son transportados por medio de la red mediante el protocolo IP usando la conmutación de paquetes y luego en el destino son nuevamente convertidos en voz estándar (Solis & Vaca, 2014).

2.4.1 Ventajas de VoIP

Dentro de las características más relevantes dentro de la VoIP, se encuentran estas como principales(Solis & Vaca, 2014)(Orquera, 2014):

- Comunicación efectiva reduciendo el costo de la llamada hasta en un 74%, y esta tarifa no depende del tiempo de conexión entre usuarios de distintos lugares.

- Tráfico de voz y datos integrado sobre el mismo acceso.
- Independencia de tecnología de transporte y del dispositivo de acceso, soportando desde teléfonos convencionales, hasta portátiles y otros dispositivos móviles.
- Escalabilidad de usuarios.
- Transmisión segura de voz, datos y video.
- Interconexión con otras redes.
- Interoperabilidad de diversos proveedores, ya que es un protocolo universal es compatible con otras redes.
- Servicios de valor añadido como correo de voz, identificador de llamadas, bloqueo de llamadas, desvío de llamadas, interacción con base de datos.

2.5 Fraude

2.5.1 Definición de Fraude

"Del latín *fraus*, un fraude es una acción que resulta contraria a la verdad y a la rectitud. El fraude se comente en perjuicio contra otra persona o contra otra organización (como el Estado o una empresa)" (Potro & Maria, 2013).

2.5.2 Fraude en Telecomunicaciones:

Dentro de las telecomunicaciones se entiende por fraude al uso deshonesto de los servicios de telecomunicaciones que perjudican los intereses de los operadores, abonados o usuarios, donde la o las personas que lo llevan a cabo no cumplen con el pago justo por el servicio utilizado (Orquera, 2014).

La evolución tecnológica en cuanto al desarrollo de la telefonía móvil y el mejoramiento de servicio de Internet, prestando anchos de banda y velocidades de trans-

misión mas alta, junto con la convergencia de servicios de telecomunicaciones, facilitan el cometimiento de fraudes ya que incrementan las posibilidades, la frecuencia y la magnitud de los delitos (Meza, 2007).

Para el 2014 el sector de las telecomunicaciones sufrió una pérdida alrededor de 4.8% del total de ingresos, es por eso que estas empresas están implementando día a día métodos de detección y control de los distintos tipos de fraude.

2.5.3 Control de Fraude

Para un correcto control de Fraude se deben seguir una secuencia de procesos, ver figura 6:

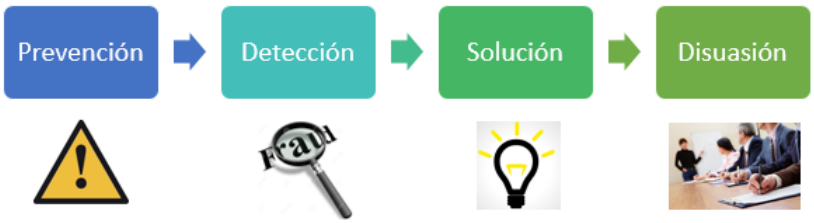


Figura 6: Diagrama Proceso de control de fraude.

Prevención: Tratar de controlar los distintos factores que pueden promover el fraude, fundamentalmente las distintas actividades de las personas que tienen acceso a la red y controlar la información confidencial que al ser de uso público puede afectar ciertos bienes o servicios.

Detección: Descubrimiento e identificación de cualquier tipo de fraude de una forma oportuna.

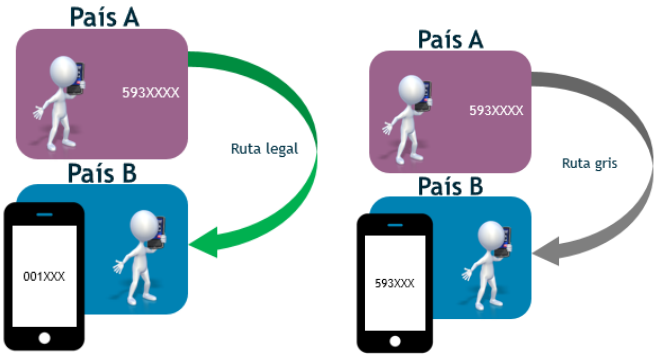
Solución: Conjunto de acciones y decisiones para contrarrestar de forma total o parcial el origen de un fraude.

Disuasión: Dar a conocer las consecuencias negativas que involucra el come-

timiento de un acto ilegal como lo es el fraude(Orquera, 2014).

2.6 Fraude ByPass

Dentro de todos los fraudes que existen el *Bypass* es el más perjudicial para los operadores de telefonía (Meza, 2007), entendiéndose por fraude *Bypass* a todo tráfico telefónico que, siendo internacional, es terminado en el país de destino como tráfico nacional. En la figura 7(a) podemos observar cómo sería la ruta normal de una llamada internacional de un país A en donde al llegar al país B se puede evidenciar que la llamada se completó correctamente ya que en la pantalla del teléfono receptor se registra un número correspondiente a un código internacional, en cambio en la figura 7(b) la llamada generada como la receptada tienen el código del mismo país.



(a) Ruta Normal. (b) Ruta Gris.

Figura 7: Definición ByPass.

Para que una llamada sea considerada como legal, la ruta que debe seguir se demuestra en la figura 8 en donde la llamada generada desde un teléfono móvil o fijo es direccionada desde un operador A por medio de un carrier hacia un operador B pero primero pasando por una central de tránsito internacional y facturándose como tal.

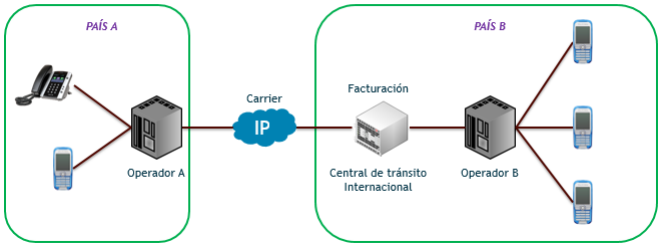


Figura 8: Ruta legal ingreso de llamada internacional.

Para el escenario de una llamada por *ByPass* el proceso inicial es el mismo, pero cuando llega al país de recepción no entra por una central de tránsito internacional sino es dirigida a una instalación clandestina no autorizada (ruta gris) y conectada al usuario final por el operador, pero facturándose como llamada nacional y no internacional.

Figura 9: Ruta ilegal ingreso de llamada internacional.

Características de un sistema "*ByPass*"(Meza, 2007) :

- Para redirigir las llamadas se utilizan varias líneas telefónicas.
- Para garantizar una calidad de servicio se requiere un enlace internacional.
- Las líneas que se utilizan para *ByPass* generan un tráfico considerable, pero no reciben llamadas con frecuencia.
- El mayor tráfico se genera cuando es fin de semana o días festivos.

- El enlace internacional es simétrico ya que se necesita el mismo ancho de banda tanto para transmisión como para la recepción, todo esto para que la calidad de servicio sea la óptima.
- Todas las líneas celulares se anclan a una misma radio base, desde donde se genera el tráfico.

2.7 OTT Bypass

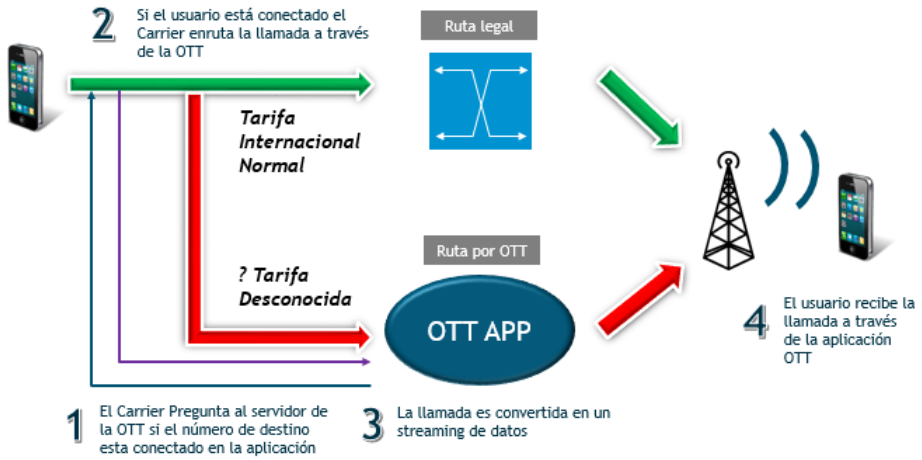


Figura 10: Diagrama OTT Bypass.

En la figura 10 se puede observar el esquema del fraude por medio de un aplicativo OTT, el cual consiste en que una llamada internacional hacia un usuario móvil no ingresa por la vía normal, es decir con un carrier autorizado el cual terminaría la llamada usando la red conmutada de la operadora del país de recepción de la llamada, sino que un carrier intermedio tiene un acuerdo con la empresa proveedora o prestadora del aplicativo OTT y comprueba si el usuario final cuenta con esta aplicación y se encuentra disponible, verificando si el número de destino se encuentra activo, la calidad de red o el ancho de banda es suficiente para ofrecer una calidad de servicio en la conexión de la llamada, si se cumple con los factores anteriormente mencionados el carrier desvía

la llamada a la aplicación OTT haciendo que la terminación sea mediante datos en la app OTT en vez de la interconexión habitual.

Aplicando este escenario a la CNT por cada minuto de llamada internacional que ingrese por medio del aplicativo Viber, CNT pierde el 100% de la tarifa que se generaría por el uso de la red conmutada normal. Todo esto sin darse cuenta ya que no hay registro alguno puesto que todo el proceso de terminación de llamada por Viber se lo realiza por medio del internet y no se registra ningún evento en la central de CNT.

2.8 Métodos de control para Fraude en Telecomunicaciones

Desarrollar métodos de prevención, detección y control de fraude por parte de las empresas dedicadas a la prestación de servicios de telecomunicaciones es necesario para el aseguramiento de sus ingresos y así disminuir las pérdidas generadas por los distintos tipos de fraude (Orquera, 2014).

2.8.1 Pruebas de lazo (loop)

Como se puede observar en la figura 11, este método consiste en realizar llamadas internacionales ya sea de forma manual o automática usando tarjetas prepago de operadores que presten los servicios de llamadas internacionales desde el país de donde se quiera identificar un posible fraude. Para el caso de *ByPass* normal el dispositivo o robot encargado de analizar los resultados de llamadas entrantes se encuentra en capacidad de filtrar las llamadas, en caso de que el número telefónico con el cual fue registrado en el identificador de llamadas se encuentre asignado a un carrier autorizado el sistema pasará por alto caso contrario si llega la llamada con un número local se contestará la llamada y generará un registro o CDR (*Call Detail Record*)de dicho evento, el mismo que posteriormente puede ser analizado para tomar acciones de identificación y disuasión del defraudador (Orquera, 2014).

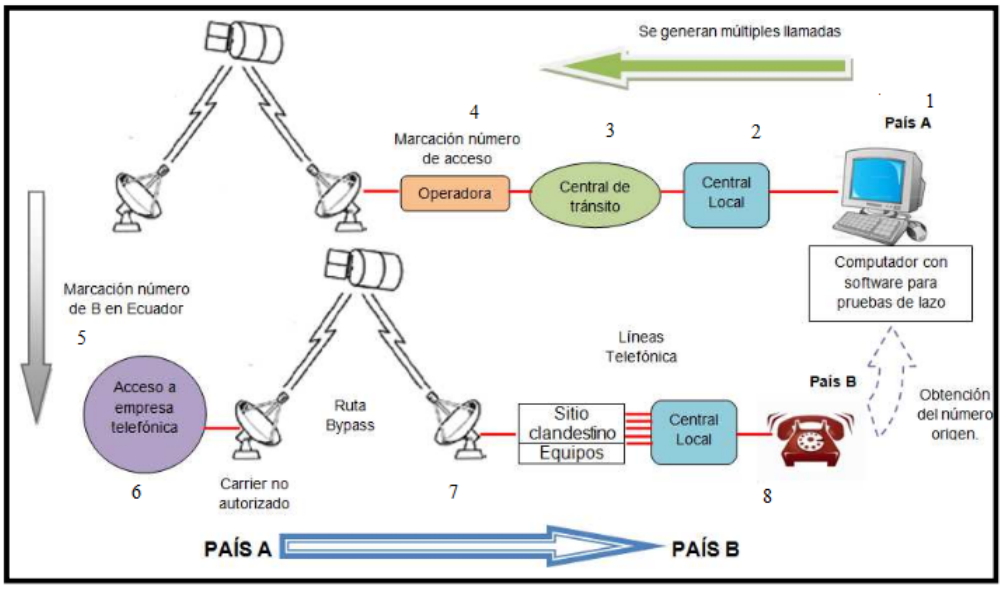


Figura 11: Diagrama pruebas de lazo.

Fuente: Orquera (2014)

Estas pruebas de lazo van de la mano con el bombardeo de llamadas el cual consiste en generar una llamada detrás de otra desde distintos de origen a varios números telefónicos que pertenezcan o sean asignados a la red de telecomunicaciones del país destino de llamada.

2.8.2 Escenario actual de pruebas para detección de fraude de la CNT EP

Actualmente la Corporación Nacional de Telecomunicaciones, tiene implementado un total de cuatro robots para la generación de llamadas de lazo, junto con un software que les permite discriminar las llamadas entrantes y realizar registro del tráfico internacional entrante, así mismo cuenta con un FMS (*Fraud Management System*), la lógica de funcionamiento de estos robots será aplicada al proyecto de investigación a desarrollarse.

No se puede detallar el funcionamiento, ni los modos de operación de dichos es-

cenarios por motivos de confidencialidad, ya que esta información es de uso exclusivo de el área de Prevención de Fraude de la CNT EP.

2.9 Sotfware

2.9.1 Base de Datos

Una base de datos es un sistema que funciona como medio de almacenamiento y organización de datos o registros, permitiendo al usuario modificar y consultar toda la información que ha sido almacenada en los registros (A. Castillo, 2015).

Dentro de las principales operaciones que un usuario puede realizar en una base de datos son:

- Añadir nueva información.
- Eliminar datos o registros existentes en la base de datos.
- Recuperar datos.
- Modificar datos.

2.9.1.1 Conceptos Básicos

- **Entidad**

  Se refiere a todo objeto que pueda ser representado y distinguido dentro de una base de datos.

- **Relación**

  Se refiere al medio de vinculación entre dos entidades, usualmente este medio es bidireccional, es decir las relaciones en ambos sentidos. Puede ser representado como un objeto ya que también puede ser considerado como entidad.

- **Atributos**

  Hace referencia a las características de una de las entidades que las definen como tal, cada entidad puede ser representada por uno o varios atributos. Como ejemplo la entidad teléfono inteligente puede estar definida por atributos como: modelo, marca, serie.

- **Cardinalidad**

  Dentro de una relación la cardinalidad hace referencia al número de entidades que tienen relación con otra entidad específica.

  Existen cuatro formas de cardinalidad:

  - **Uno a uno:** Una entidad se relaciona solo con otra entidad específica.
  - **Uno a Varios:** Una entidad se relaciona con varias entidades.
  - **Varios a Uno:** Varias entidades se relacionan con una sola entidad.
  - **Varios a Varios:** Varias entidades se relacionan con varias entidades

2.9.1.2 Modelo conceptual de una base de datos (CDM)

Es el diagrama inicial del cual se parte para el diseño de una base de datos, es decir muestra una estructura básica de cómo va a ser conformada la base sin mostrar mayor detalle. Es primordial que este modelo se encuentre correctamente elaborado ya que de lo contrario la base de datos podría ocasionar problemas (A. Castillo, 2015).

Dentro del modelo conceptual se presentan únicamente las entidades, su relación y su cardinalidad.

2.9.1.3 Modelo físico de una base de datos (PDM)

Este modelo presenta una descripción de cómo se encontrará almacenada y organizada la información de la base de datos. Toma como punto de inicio modelo concep-

tual, añadiendo a este todas las tablas y atributos que deben estar presentes (A. Castillo, 2015).

Mediante este modelo el desarrollador cuenta con una estructura real de la base datos.

2.9.2 MySQL

Es un sistema que funciona como un gestor de bases de datos, es uno de los más populares en el mundo y se estima que se han distribuido alrededor de 100 millones de copias del software a lo largo de la historia (A. Castillo, 2015).

Dentro de las ventajas principales de este sistema se tienen:

- Portabilidad.
- Código Fuente con alta disponibilidad.
- Gratuito.
- Desempeño óptimo.
- Fácil manejo por parte del usuario.

2.9.2.1 SQL

Es el lenguaje sobre el que está basado MySQL, este lenguaje está diseñado para el acceso a las bases de datos ya que permite realizar consultas, inserción, modificación o eliminación de registros. Se basa en declaraciones, es decir expone lo que requiere obtener, mas no como obtenerlo(A. Castillo, 2015).

Las sentencias principales de este lenguaje son:

- ***SELECT:*** Permite consultar los registros almacenados en la base de datos.
- ***INSERT:*** Permite el ingreso de nuevos registros a la base de datos.

- ***UPDATE:*** Permite modificar los registros existentes en la base de datos.
- ***DELETE:*** Elimina registros de una base de datos.

2.9.3 Lenguaje PHP

PHP es un lenguaje de programación abierto, el mismo que se encuentra orientado para su uso en servidores y desarrollo Web. Dentro de aplicaciones con código HTML se puede introducir código PHP el mismo que se ejecutará cada vez que un usuario acceda a la página Web (A. Castillo, 2015) .

PHP se basa enteramente en código abierto lo cual permite tener un acceso total al código fuente, modificarlo y distribuirlo libremente.

Las ventajas principales de este lenguaje son:

- Portabilidad.
- Gratuito.
- Interfaces compatibles con la mayoría de sistemas gestores de bases de datos.
- Uso relativamente amigable con el desarrollador.
- Librerías ya implementadas para tareas simples.

PHP es un lenguaje eficiente, usando únicamente un servidor web es posible procesar una gran cantidad de visitas por día. Además, dado que fue diseñado para la creación de sitios web, posee varias herramientas útiles incorporadas. Ejemplos de estas herramientas son: generar imágenes GIF, conectar con otros servicios de red, generar documentos e incluso enviar *emails* (A. Castillo, 2015).

Se escogió estos lenguajes de programación principalmente por ser software gratuito, además de ser muy robustos en cuanto a funcionalidad y compatibilidad ya que

sus librerías vienen ya con tareas implementadas, en la red se encuentra mucha información para su desarrollo y como se pueden integrar unos con otros facilitando así la realización de un proyecto.

CAPÍTULO 3

DISEÑO Y DESARROLLO

3.1 Estructura del sistema.

El sistema de detección de OTT *Bypass* por medio del OTT Viber desarrollado sobre la plataforma Android toma como punto de inicio la generación de llamadas de lazo, método con el cual se ha detectado y controlado el fraude *Bypass*.

El sistema posee tres partes principales:

1. Funcionando como un generador de llamadas.
2. Como receptor de llamadas.
3. Como aplicación Web para el procesamiento de la información y emisión de informes.

El teléfono inteligente que funciona como generador de llamadas tiene dos funciones principales: a) Almacenar dentro de una base de datos en el servidor los datos necesarios para la ejecución de un proceso de llamadas de lazo, b) Realizar el proceso de llamadas de lazo, permitiendo escoger al usuario la cantidad de llamadas y con qué tipo de tarjetas quiere realizar este proceso.

El teléfono inteligente que funciona como receptor de llamadas recogerá por medio de una ventana de navegador los datos de los registros de llamadas entrantes tanto por la red conmutada de CNT y por el OTT Viber.

Finalmente, en la aplicación web por medio del servidor los resultados provenientes tanto del teléfono generados como del teléfono receptor serán analizados y se presentarán al usuario en un informe detallado en formato .pdf.

Para las conexiones de los teléfonos móviles que funcionan como receptor y generador de llamadas con el servidor se ha usado un modelo tipo Cliente-Servidor, permitiendo así que dos o más dispositivos móviles interactúen con un único servidor, el mismo que proporcionará los datos necesarios para el correcto funcionamiento del sistema en sus distintos modos o funciones. En la figura se muestra la estructura del sistema bajo este modelo.

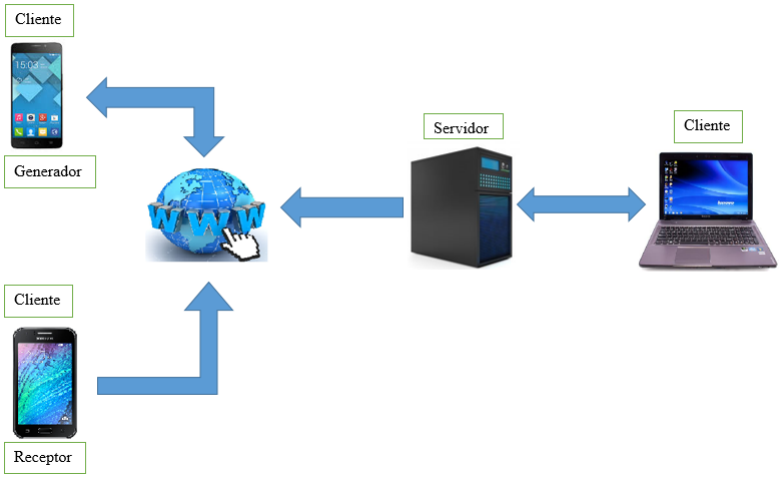


Figura 12: Diagrama Cliente-Servidor.

Los componentes principales del sistema son:

- Aplicación móvil desarrollada para dispositivos Android desde la versión 4.1 en adelante, que se encuentra en el teléfono generador de llamadas.
- Aplicación Web desarrollada usando plantillas *Bootstrap* para mejorar el acoplamiento

a cualquier tamaño de pantalla de dispositivos y con código PHP, alojada en el servidor Web contratado.

- Base de datos MySQL, alojada en el servidor Web contratado.

3.1.1 Requerimientos

El sistema debe cumplir con cuatro funciones principales:

1. Almacenar y obtener todos los parámetros requeridos para la ejecución de llamadas de lazo.
2. Obtener un registro de llamadas salientes y entrantes ya sea por la red conmutada de CNT o por el OTT Viber.
3. Ser capaz de enviar esta información del registro a un servidor donde será almacenada en una base de datos.
4. Presentar informes con la información recopilada durante las pruebas.

Para la ejecución de llamadas de lazo como se observa en la tabla 1 se identificaron los siguientes parámetros realizando pruebas manuales con cada tarjeta que deberá usar el aplicativo para la ejecución del bombardeo con las llamadas de lazo:

Tabla 1:

Parámetros Requeridos.

Parámetro	Tipo	Descripción
Identificador	Obligatorio	Nombre de la tarjeta o identificativo con el cual se asociarán posteriormente todos los datos de los campos posteriores a este.
Salida	Obligatorio	Es el código de salida del país de origen de la llamada. Ejemplo: EE.UU=001.
Tarjeta	Obligatorio	Es el número o IVR (Interactive Voice Response) de la empresa proveedora del servicio de llamadas internacionales.
Idioma	Opcional	Este campo es opcional ya que se lo debe llenar solo en caso de que la configuración de la tarjeta requiera selección de idioma para continuar con la secuencia.
Pin	Obligatorio	Número pin de la tarjeta que se va a utilizar para las llamadas.
Entrada	Obligatorio	Es el código de entrada desde el país que se realiza la prueba hacia el país donde se encuentre el teléfono receptor. Ejemplo: Desde España a Ecuador= 00
Destino	Obligatorio	Es el número del chip del teléfono receptor. Ejemplo: 593982094954

Adicionalmente se identificó que para la llamada se ejecute de forma correcta se debe seguir una secuencia específica de marcado o de ingreso de estos parámetros para esto de deben realizar unas pausas:

Tabla 2:

Parámetros Requeridos.

Parámetro	Tipo	Descripción
Tiempo Idioma	Obligatorio	Es el tiempo en segundos que debe esperar desde que se conecta la llamada hasta que pide ingresar la opción de idioma.
Tiempo Pin	Obligatorio	Es el tiempo en segundos desde que se ingresa la opción idioma o desde que se conecta la llamada
Tiempo destino	Obligatorio	Es el tiempo en segundos desde que se ingresa la opción de Pin.

3.1.1.1 Requerimientos del aplicativo móvil:

Para que se puedan recopilar todos los datos necesarios y realizar correctamente las pruebas las funciones que debe cumplir el aplicativo móvil en el teléfono generador son:

- Bombardeo de llamadas hacia el teléfono receptor desde los principales países desde donde se hacen las pruebas: Estados Unidos, España e Italia. Permitiendo que el proceso de llamadas se genere continuamente y contemple algunas restricciones para el uso de varias tarjetas de forma consecutiva.
- Posibilidad de configurar una nueva tarjeta de prueba, con los respectivos tiempos de espera para la rutina de marcado.
- Extracción y tabulación de los archivos con los registros de las llamadas en el sistema operativo Android.

- Posibilidad de comunicarse con el servidor para la ejecución de las distintas funcionalidades del sistema.

3.1.1.2 Requerimientos del aplicativo Web:

El aplicativo Web debe cumplir con los siguientes requerimientos:

- Manipulación de tarjetas: el aplicativo debe proporcionar al usuario la posibilidad de ingresar una nueva tarjeta con todos los parámetros necesarios, buscar una tarjeta en específico, borrar del sistema tarjetas caducadas o sin saldo.
- Búsqueda de resultados: el usuario puede buscar eventos Viber por medio de la fecha específica del día que las pruebas se hayan almacenado en el servidor.
- Presentación de resultados: Los resultados obtenidos de las pruebas con bombardeo de llamadas deben presentarse en un informe detallado con la fecha del día que se requiera el informe.

3.1.2 Herramientas y recursos

Para la implementación del sistema se utilizó un teléfono inteligente Alcatel Idol 3 con sistema operativo Android 4.1 y posibilidad de conexión a la red 4G o LTE. Y un teléfono inteligente Samsung J1 Ace con sistema operativo Android 4.1 y posibilidad de conexión a la red 4G o LTE.

3.2 Desarrollo de la aplicación móvil para la generación de llamadas.

Para la programación de la aplicación móvil se usó el programa Android Studio en su versión 2.0, permitiendo escoger desde que versión de sistema operativo funcionará, en este caso se seleccionó que funcione a partir de la versión Android 4.1 *Jelly Bean*,

dado que es la versión instalada de fábrica que contenían los teléfonos de pruebas. Se presenta en la figura el diagrama de bloques del sistema:

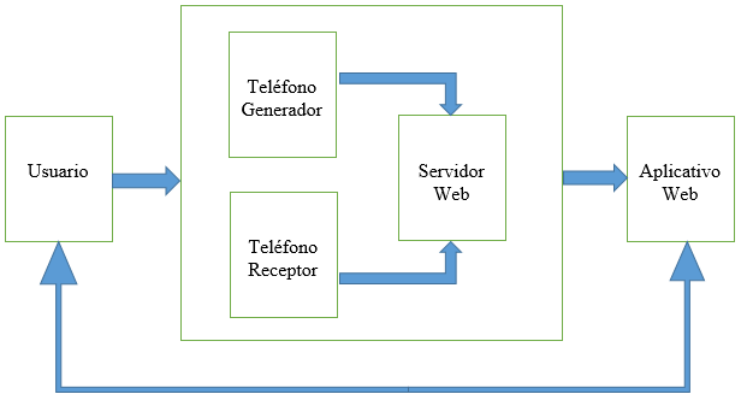


Figura 13: Diagrama de bloques del sistema.

3.2.1 Modos de funcionamiento de la Aplicación Móvil

El aplicativo móvil de acuerdo a los requerimientos consta de dos modos de funcionamiento, el primero como generador de llamadas de lazo o *Loop* de llamadas, y el segundo como almacenador de nuevas tarjetas.

3.2.1.1 Diagramas UML(*Unified Modeling Language*)

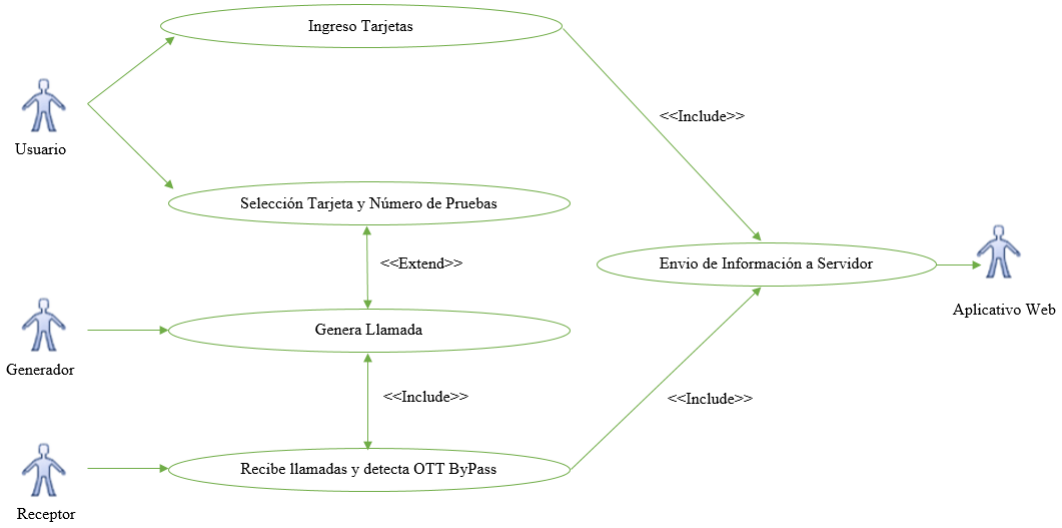


Figura 14: Diagrama UML casos de uso.

El diagrama UML para los casos de uso nos presenta cuatro actores principales el usuario, el generador de llamadas, el receptor de llamadas y el servidor con la aplicación Web que permitirá la presentación de la información del funcionamiento y resultados del aplicativo móvil del generador y receptor de llamadas. El usuario se encarga del ingreso de tarjetas que a su vez se encuentra directamente relacionado con el envío de información hacia el servidor, ya que el usuario ingresará todos los campos requeridos para posteriormente realizar el Loop de llamadas.

Si se selecciona el modo de funcionamiento de lazo, el usuario seleccionará con que tarjetas quiere trabajar y decidirá cuantas pruebas realizará, y así tanto el generador como el receptor enviarán sus registros al servidor donde la aplicación web tabulará los resultados para finalmente presentar los datos de forma ordenada de todos los eventos de OTT Viber que hayan suscitado dentro de la ejecución de las pruebas.

La aplicación desarrollada está compuesta de siete clases las cuales se presentan en el diagrama UML de clases en la figura 15 , y las mismas que serán detalladas a continuación.

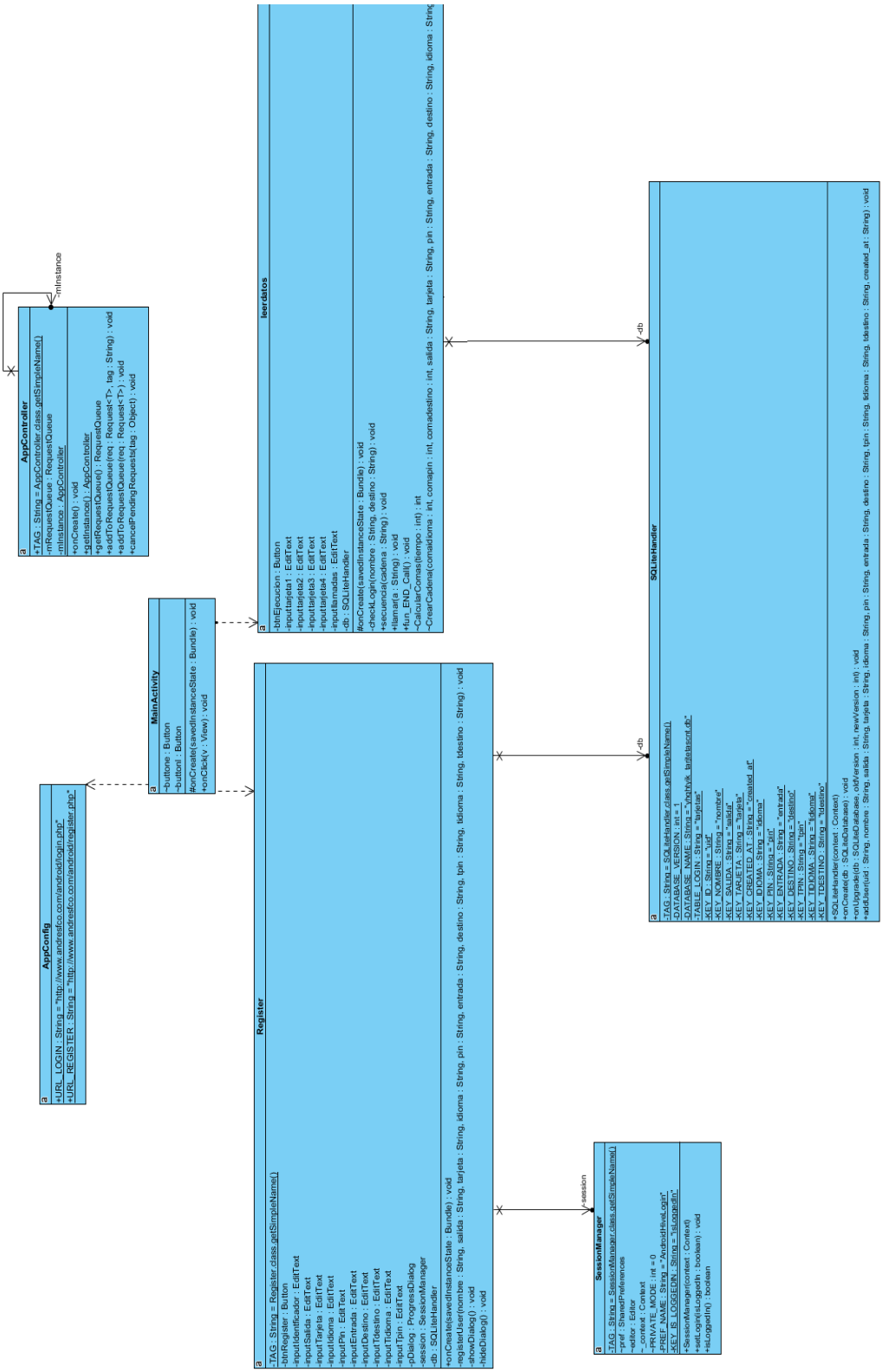


Figura 15: Diagrama UML de Clases .

3.2.2 Interfaz de usuario del aplicativo móvil.

Para que el sistema cumpla con un desempeño óptimo se procuró que se cumplan estos tres criterios:

- Interfaz Instintiva.
- Fácil manejo y comprensión.
- Ejecución Coherente.

La conectividad con el servidor es la base de la ejecución ya que para ambos modos de funcionamiento se requieren datos almacenados en el servidor, en caso de no contar con conexión al servidor o faltar algún parámetro se presentará un mensaje de error y la ejecución no se completará.

En la figura 16(a) se muestra el diseño de la ventana principal, la cual se presentará al usuario al ingresar al aplicativo, mientras que en la figura 16(b)se muestra la ventana ya implementada.

(a) Diseño ventana principal. (b) Ventana principal implementada.

Figura 16: Ventana Principal.

En la tabla 3 se muestra la descripción de cada componente de la ventana inicial.

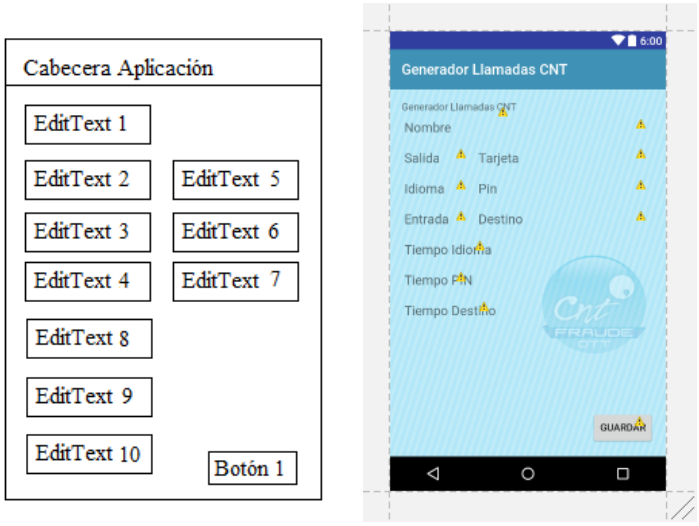
Tabla 3:

Componentes ventana principal.

Componente	Descripción
Botón 1	Permite el acceso a la ventana de almacenamiento de tarjetas.
Botón 2	Permite el acceso a la ventana de ejecución del Loop de llamadas.

En caso de seleccionar el modo de almacenar una tarjeta el programa nos redirigirá a otra ventana en donde se podrá ingresar todos los parámetros necesarios para un completo registro de una tarjeta en la figura 17(a) se presenta el diseño de la ventana

con todos sus componentes mientras que en la figura 17(b) se presenta la ventana ya implementada.



(a) Diseño ventana almacenar. (b) Ventana almacenar implementada.

Figura 17: Ventana Almacenar.

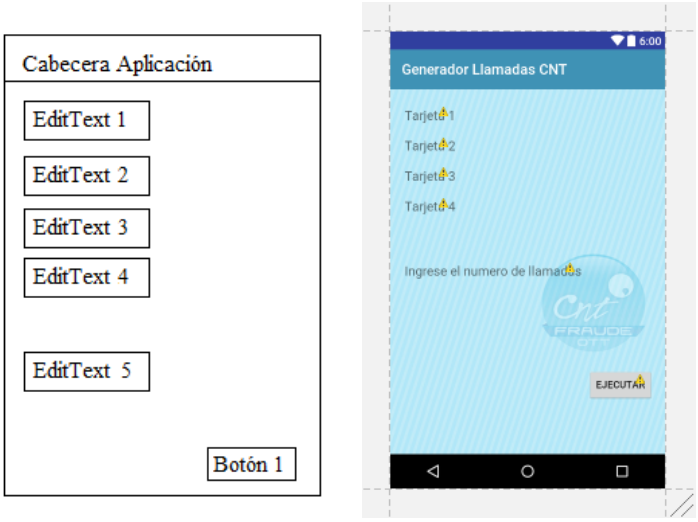
En la tabla 4 se muestra la descripción de cada componente de la ventana almacenar.

Tabla 4:

Componentes ventana almacenar.

Componente	Descripción
EditText 1	Se utiliza para el ingreso del nombre de la tarjeta.
EditText 2	Se utiliza para el ingreso del código de salida de la tarjeta.
EditText 3	Se utiliza para el ingreso de la opción idioma.
EditText 4	Se utiliza para el ingreso del código de entrada al país de destino.
EditText 5	Se utiliza para el ingreso del número o IVR de la tarjeta.
EditText 6	Se utiliza para el ingreso del Pin de la tarjeta.
EditText 7	Se utiliza para el ingreso del número receptor o de destino.
EditText 8	Se utiliza para el ingreso de la variable Tiempo Idioma.
EditText 9	Se utiliza para el ingreso de la variable Tiempo Pin.
EditText 10	Se utiliza para el ingreso de la variable Tiempo Destino.
Botón 1	Envía los parámetros ingresados para almacenarse en el servidor.

En caso de seleccionar la segunda función o segundo modo de uso de la aplicación móvil, se desplegará la ventana cuyo diseño se muestra en la figura 18(a) y su implementación se encuentra en la figura 18(b).



(a) Diseño ventana llamar.

(b) Ventana llamar implementada.

Figura 18: Ventana Llamar.

En la tabla 5 se muestra la descripción de cada componente de la ventana ejecutar.

Tabla 5:

Componentes Ventana Ejecución.

Componente	Descripción
EditText 1	Se utiliza para el ingreso del nombre de la tarjeta 1.
EditText 2	Se utiliza para el ingreso del nombre de la tarjeta 2.
EditText 3	Se utiliza para el ingreso del nombre de la tarjeta 3.
EditText 4	Se utiliza para el ingreso del nombre de la tarjeta 4.
EditText 5	Se utiliza para el ingreso del número o cantidad de llamadas que el programa ejecutará.
Botón 1	Permite el inicio de la ejecución del Loop de llamadas.

3.3 Comunicación con el servidor.

La función principal que debe cumplir el aplicativo móvil es el establecimiento de la conexión con el servidor, para así realizar el intercambio de información, tanto en el modo de registro de tarjetas como en el modo de ejecución de lazo de llamadas, en el caso de que no exista conexión a internet no se podrá ejecutar el aplicativo y presentará al usuario un mensaje de conexión inexistente.

Para lo cual se han definido las siguientes clases:

3.3.1 Clase AppConfig

Esta clase se encarga de almacenar el dominio en donde se encuentra almacenado el servidor y hacia las cuales apuntará nuestra aplicación tanto para el envío como para la recepción de la información desde y hacia el servidor.

3.3.2 Clase AppController

Permite iniciar el requerimiento para establecer la conexión con el servidor. Habilitando a la aplicación para estar en constante escucha y petición. Funciona de forma que la conexión con el servidor siempre se encuentre activa.

3.4 Almacenamiento temporal de los elementos

El proceso en ambas funciones del aplicativo móvil requiere de los mismos parámetros para su ejecución, para esto mientras en el modo de almacenamiento se recogen todos los parámetros para ser enviados hacia el servidor, en el modo generación de llamadas se receptan desde el servidor hacia el teléfono generador los mismos parámetros que se almacenan de forma temporal en el teléfono generador hasta que se ejecute nuevamente cualquiera de los dos procesos .

3.4.1 Clase Session Manager

Cada vez que se ejecute el proceso de requerimiento de un almacenamiento temporal de todos los parámetros de las tarjetas, se activará esta clase cuya funcionalidad es acceder a la base de datos que se crea temporalmente en el dispositivo móvil, proporcionando permisos de administrador para que se pueda almacenar o modificar los registros de esta base.

3.4.2 Clase SQLiteHandler

Cuando un proceso se ejecuta, se realiza la declaración y creación de una base de datos siempre con el mismo nombre y los mismos atributos, que se requiere tanto para la función almacenar como para la función ejecutar, asignando cada variable dependiendo del nombre y el valor que se le asigne a esta variable.

3.5 Selección del modo de funcionamiento

El usuario al iniciar la aplicación móvil debe poder escoger el modo de funcionamiento de la aplicación, para ello se presenta en una ventana principal (figura 19) la posibilidad de la selección, la clase encargada de permitir esto al usuario se la ha tomado como la clase principal:

Figura 19: Ventana Principal.

3.5.1 Clase MainActivity

En esta clase se encuentra implementado un método cuya función es determinar que selección hizo el usuario y así redirigir a las clases que cumplan con el requerimiento del usuario.

En el método onCreate se le asigna a cada botón una variable o identificativo único el cual servirá para que en el método onClick se pueda determinar que botón fue pulsado y así se pueda redirigir a la ventana de la clase correspondiente a cada modo de ejecución.

3.6 Almacenar Tarjetas

El primer modo de uso de la aplicación móvil se encuentra delimitado para el ingreso de nuevos registros con los parámetros que se requiere de una tarjeta para que posteriormente esta sea utilizada para ejecutar el Loop de llamadas.

3.6.1 Clase Register

En esta clase se toman todos los parámetros que el usuario ha ingresado en los EditText de la pantalla correspondiente al modo de funcionamiento almacenar. Se procesa todos estos parámetros y se los almacena en un objeto de tipo JSON (*Java Script Object Notation*), y finalmente se los envía a guardar en el servidor.

Primeramente, a cada parámetro se le asigna una variable única de tipo *private* y dentro del método onCreate se le asigna la identificación correspondiente a cada elemento de la ventana de almacenar tanto a los EditText como al botón, se comprueba la conexión con el servidor.

Al momento de presionar el botón, a cada EditText se lo convierte en String, para poder usar la información que contiene cada EditText y así por el método tipo void

denominado registerUser se almacena cada parámetro como parte del elemento JSON que será enviado hacia el servidor para almacenarse posteriormente.

3.7 Ejecución del Loop

Este modo de uso permite al usuario seleccionar con que tarjetas quiere realizar las llamadas y la cantidad de veces que el programa ejecutará este proceso.

3.7.1 Clase leerdatos

Está clase toma el contenido de cada uno de los elementos de los EditText puestos en la ventana correspondiente a este proceso y los trata de forma diferente, por un lado, se encuentran los nombres de cada tarjeta y por otro la cantidad de llamadas que se ejecutará el proceso.

Con los nombres de la tarjeta se podrán extraer los parámetros requeridos para la correcta ejecución de las llamadas y con la cantidad de llamadas se le especifica al programa cuantas veces debe realizar la secuencia de marcado. Como primer paso se ejecuta un aleatorio para poder escoger al azar una tarjeta diferente para cada ejecución en caso de que la tarjeta no coincida con la almacenada en el servidor el programa presentará una alerta, caso contrario se proseguirá con la ejecución normal.

Mediante el método de tipo void denominado secuencia se procede a realizar la ejecución de la llamada y las pausas necesarias entre llamada y llamada, al ser un bucle de llamadas se ha definido un tiempo de 80 segundos por ejecución. Al cumplirse este tiempo el método fun_END_Call es llamado para cortar la llamada, espera un tiempo de 9 segundos y vuelve a iniciar con la secuencia hasta llegar al máximo que es el número que el usuario estipuló en el EditText correspondiente al número de llamadas.

3.8 Implementación del Servidor

Una parte muy importante del proyecto de investigación es la creación de un servidor que permita visualizar de forma ordenada los eventos de OTT Viber ocurridos durante la ejecución de cada ciclo de pruebas, para esto se requiere que el servidor aloje cada uno de los datos de los eventos, así como cada uno de los parámetros que requiere la aplicación móvil para ejecutarse.

3.8.1 Diseño de la base de datos

Para la ejecución del Loop de llamadas y la presentación de resultados se diseñó una base de datos que almacene la información de las tarjetas, así como las llamadas entrantes por la red conmutada o por el aplicativo Viber. La base de datos diseñada se denomina CNT y está formada por cinco tablas: llamadasentrantes, llamadasgeneradas, tarjetas, usuarios, Viber.

3.8.1.1 Tabla llamadasentrantes

En la tabla llamadasentrantes se almacena todas las llamadas que han ingresado por medio de la red conmutada de la CNT EP. Consta de cuatro campos: identificador, número, hora y fecha. El identificador primario o *primary key* será la variable denominada indentificador ya que será el único parámetro que no se repetirá. Además, la variable identificador al ser de aumento progresivo permitirá contabilizar la totalidad de llamadas recibidas, lo cual es muy importante para la cuantificación de los resultados y posterior análisis de los mismos.

3.8.1.2 Tabla llamadasgeneradas

En esta tabla se almacenarán todas las llamadas que han sido ejecutadas por el generador. Consta de cuatro campos: identificador, número, fecha y hora. El identificador primario o *primary key* será la variable denominada identificador ya que es el único

parámetro que no se repetirá ya que cada evento se guarda con un identificador diferente.

3.8.1.3 Tabla tarjetas

Contiene toda la información requerida para la ejecución de las llamadas. Consta de 12 campos: uid, nombre, salida, tarjeta, idioma, pin, entrada, destino, tidioma, tpin, tdestino, created_at, siendo el identificador primario o *primary key* el campo denominado uid ya que cada tarjeta que se registre se le asignará un único uid.

3.8.1.4 Tabla usuarios

Esta tabla contiene la información de las personas que pueden acceder al sistema para consultar, insertar o borrar cualquier información contenida en las otras tablas. Consta de tres campos: ident, nombre y password. Siendo el identificador primario ident ya que cada usuario posee un identificador único que es asignado al momento de que se crea un nuevo usuario.

3.8.1.5 Tabla viber

Contiene cada uno de los eventos de potencial Bypass por medio del OTT Viber, siendo estos todas las llamadas que ingresaron por el aplicativo Viber y no por la red conmutada de la operadora. Contiene cuatro campos: identificador, fecha, hora, ivrnumero. El identificador primario es indentificador ya que el sistema asigna automáticamente al momento de ingresar un evento y es irrepetible.

3.8.2 Servidor Web para la aplicación

La aplicación del servidor fue programada enteramente en lenguaje PHP por lo tanto las pruebas de funcionamiento se las hicieron de forma local usando el software XAMPP, este software permite que un computador sirva como servidor web local.

Pero dado que la aplicación requería conexión remota al servidor y este debía estar disponible en cualquier locación se usó un servidor externo pagado.

Se usó un servidor web de la empresa Yamburara, permitiendo así adquirir el dominio www.andresfco.com, brindando las siguientes características:

- 2GB de almacenamiento.
- 20GB de transferencia.
- 1 dominio predeterminado.
- Gestión del sitio mediante cPanel.

Para realizar la conexión con el nuevo servidor se debió actualizar los parámetros de conexión con los siguientes valores:

Tabla 6:

Valores de parámetros de conexión.

Parámetro	Valor
Nombre del servidor web	localhost
Nombre de la Base de Datos	yhqhtyik_CNT
Usuario	yhqhtyik
Clave	yhqhtyik

El nombre del servidor no ha cambiado ya que todos los archivos que forman parte del aplicativo se encuentran almacenados dentro del dirección raíz o directorio local. Para que todos los procesos se encuentren correctamente establecidos y funcionales es necesario subir el resto de los archivos con extensión .php, para esto se usó el software libre para cliente FTP denominado FileZilla.

Luego de culminar el proceso ya se pueden enviar y receptar los datos desde el receptor al dispositivo móvil y viceversa sin necesidad que se encuentren ambos perteneciendo a una mima red LAN, permitiendo así la portabilidad del sistema.

CAPÍTULO 4

PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA

4.1 Funcionamiento de la aplicación móvil.

Se desarrolló un aplicativo compatible con el 95.2% de los dispositivos móviles que tienen sistema operativo Android a partir de la versión 4.1 (*Jelly Bean*) con API 16 en adelante (Developer, 2016). Por motivos de pruebas y cambio de escenarios el aplicativo se instaló en distintos dispositivos móviles y funcionó correctamente.

Las pruebas de funcionamiento que se realizaron consistieron en:

- Comprobar que la aplicación funciona correctamente tanto con conexión SMA como con conexión WiFi.
- Verificar que la interfaz gráfica fue diseñada para dispositivos de pantalla Media-Grande, haciendo que los elementos no se distorsionen al cambiar de dispositivo móvil.
- Validar que la conexión y parámetros de envío con el servidor para el intercambio de la información son las correctas.

- Determinar que la aplicación se ejecuta de forma normal y consecutiva sin sufrir retrasos dentro de la ejecución de llamadas de lazo.

Tabla 7:

Pruebas de Funcionamiento de la Aplicación Móvil.

Android	Dispositivo	Conexión	Interfaz	Validación	Diagnóstico
4.2.2	LG Flex	Ok	Ok	Ok	Ok
5.0	Alcatel Idol 3	Ok	Ok	Ok	Ok
5.1.1	J1 Ace	Ok	Ok	Ok	Ok

4.2 Funcionamiento de la aplicación Web.

Para comprobar el correcto funcionamiento del aplicativo Web se ejecutaron las llamadas de lazo y se registraron nuevas tarjetas. Los resultados de estas pruebas fueron enviados y almacenados en la base de datos del servidor con el fin de verificar que no existe pérdida de datos. Para esto se realizaron cinco pruebas visibles en la tabla 8 las cuales consistieron en:

- **Prueba 1:** Se almacenó en la base de datos el registro de llamadas generadas, llevando en cada prueba cada campo necesario para la correcta tabulación.
- **Prueba 2:** Se almacenó en la base de datos el registro de llamadas entrantes por la red conmutada de la Corporación Nacional de Telecomunicaciones CNT EP.
- **Prueba 3:** Se almacenó en la base de datos el registro de llamadas entrantes por el aplicativo Viber.
- **Prueba 4:** Se realizó el registro de una nueva tarjeta ingresando todos los parámetros requeridos desde el aplicativo móvil.

- **Prueba 5:** Se realizó el registro de una nueva tarjeta ingresando todos los parámetros requeridos desde la aplicación Web.

Tabla 8:

Pruebas de Funcionamiento de la Aplicación Web.

Parámetro	Prueba 1	Prueba 2	Prueba 3	Prueba 4	Prueba 5
Enviados	3	3	3	2	2
Recibidos	3	3	3	2	2
Eficiencia	100%	100%	100%	100%	100%

4.3 Protocolos de Prueba

El sistema desarrollado posee dos modos de funcionamiento: registro de nuevas tarjetas y generador de llamadas de lazo, para los cuales se realizó las pruebas de funcionamiento respectivas que se detallan a continuación.

4.3.1 Registro de Tarjetas.

En el modo de registro de tarjetas, se almacenó un aproximado de 40 tarjetas en el periodo de diciembre 2015 a mayo 2016, el mismo que se detalla en la tabla 9. Las pruebas correspondientes permiten comprobar el correcto funcionamiento del servidor a través del establecimiento de comunicación de modo aleatorio a distintas horas del día y en varios escenarios de conexión inalámbrica como WiFi, 2G, 3G o 4G.

Como se puede evidenciar en la 9 se han probado solo tarjetas prepago provenientes de Estados Unidos, esto debido a la disponibilidad de dichas tarjetas por parte del departamento técnico de la Jefatura de prevención de fraude de la CNT, pero el sistema se encuentra en la posibilidad de ingresar tarjetas de otros países como España e Italia.

Tabla 9:

Tarjetas Ingresadas.

Nombre	Cantidad	IVR
Check	2	3472738005
Rosita	2	5164530129
Colombia	4	2014929053
Anisiya	5	6466015070
Dinamita	3	5186499988
Mágica	5	5854712713
Chris	5	9143721942
Hotlina	3	6315260100
Otra	5	6317878349
Nobel	3	6467571378
Notebook	3	5167349886
Total	40	

4.3.2 Generador de Loop de llamadas.

El generador de llamadas de lazo plantea tres escenarios para su ejecución: el primero a través de la variación de tecnología SMA (Sistema Móvil Avanzado), que permite llevarlo a cabo en las formas de conexión a internet: 2G, 3G y 4G. El segundo con la variación de conexión wi-fi, por medio del uso de los proveedores del servicio de internet: Netlife, TVCable y la Corporación Nacional de Telecomunicaciones CNT EP. Y por último el escenario generado a través de la variación de operadora de red: Movistar y Claro. Las pruebas realizadas se hicieron en un mínimo de 500 y un máximo de 900 en el lapso de 24 horas, siendo factor determinante para estos valores el tiempo de ejecución entre llamadas de lazo. Para la realización de las pruebas se usó como receptor del bombardeo de llamadas el teléfono inteligente Alcatel Idol 3,

debido a que permitió el acceso a todas las bandas de conexión desde 2G hasta 4G, que ofrece la Corporación Nacional de Telecomunicaciones CNT EP. El análisis de las pruebas se basó tanto en los parámetros de conexión a internet como en los resultados obtenidos.

4.3.2.1 Pruebas a través de Tecnología SMA.

La variación de tecnología SMA consiste en modificar el tipo de conexión a distintos anchos de banda, forzando al teléfono receptor a adoptar un solo modo de conexión durante el tiempo de realización de las pruebas. Para la aplicación de este método se usó el servicio de datos de la Corporación Nacional de Telecomunicaciones CNT EP, en las tecnologías 2G, 3G, 4G.

- **Tecnología 2G.-** Trabaja en la banda de los 800 a 900 Mhz, con una velocidad de transmisión inicial de 9.6 kbps, la cual a través de mejoras realizadas en la última década a permitido alcanzar una velocidad de transmisión desde 56kbps a 150kbps (Barreno, Carrión, & Mejía, 2016).

  En la ejecución de las pruebas con la conexión 2G, se programó al generador para que realice un total de 1000 llamadas, siendo las recibidas 623, constituyendo una eficiencia del sistema de 62.3%. Ver tabla 10.

Tabla 10:

Llamadas 2G.

Tipo de llamadas	Cantidad
Generadas	1000
Recibidas	623
No Completadas	377
Eficiencia	62.3%

De las 623 llamadas completadas exitosamente, entraron un total de 0 lla-

madas por medio del aplicativo Viber. Ver tabla 11. Esto se podría explicar a través del hecho de que el ancho de banda de la red 2G no cumple con los requerimientos técnicos del aplicativo Viber para terminación de llamada.

Tabla 11:

Llamadas Completadas 2G.

Llamadas Completadas	Cantidad
Red conmutada CNT	623
Viber	0

- **3G o H+ .-** Esta tecnología trabaja en las mismas bandas de frecuencia que la red 2G. En esta tecnología convergen los servicios de voz y datos, alcanza una velocidad de 384 kbps con el usuario movilizándose a 120km/h y 2 Mbps a 10km/h. Una generación intermedia es HSPA o H+, con velocidades de 14.4 Mbps en enlace descendente y 5.8 Mbps en enlace ascendente (Barreno et al., 2016).

  En la tabla 12 se presenta la realización de pruebas con conexión 3G, donde se programó al generador para que realice un total de 2500 llamadas, siendo las recibidas 2103, representando una eficiencia de 84.12%.

Tabla 12:

Llamadas 3G o H+.

Tipo de llamadas	Cantidad
Generadas	2500
Recibidas	2013
No Completadas	397
Eficiencia	84.12%

De las 2013 llamadas recibidas, 2005 ingresaron por la red conmutada de la Corporación Nacional de Telecomunicaciones CNT EP, y 8 a través del aplicativo Viber correspondiendo a un 0.39%. Ver tabla 13.

Tabla 13:

Llamadas Completadas 3G o H+.-.

Llamadas Completadas	Cantidad
Red conmutada CNT	2005
Viber	8

- **4G .-** Esta es la última generación implementada en el Ecuador, se encuentra basada en tecnología IP, con velocidades de 20488.69 Kbps en enlace descendente y 3662,31 Kbps en enlace ascendente (Cevallos & Ortiz, 2016), trabajando en las bandas de 700 Mhz, AWS (1.700/2.100 Mhz) y 2,5 Ghz, según lo detalla la resolución del Conecel (Universo, 2015).

  En el escenario de pruebas realizadas con conexión 4G se programó al generador para que ejecute 3891 llamadas, de las cuales 2250 fueron las recibidas, constituyendo un 57,82% de eficiencia, valor bajo en comparación con las pruebas con conexión 2G y 3G, probablemente debido a que las tarjetas de prueba se hallaban en condiciones caducas o sin saldo disponible. Ver tabla 14.

Tabla 14:

Llamadas 4G.

Tipo de llamadas	Cantidad
Generadas	3891
Recibidas	2250
No Completadas	1641
Eficiencia	57.82%

La tabla 15 evidencia 63 llamadas que ingresaron por medio del aplicativo Viber, del total de 2250 recibidas en el escenario 4G, correspondiendo al 2.8% de llamadas recibidas.

Tabla 15:

Llamadas Completadas 4G.

Llamadas Completadas	Cantidad
Red conmutada CNT	2187
Viber	63

4.3.2.2 Variación de Operadora

Para proceder con estas pruebas se hizo uso de la red 4G de las operadoras Movistar y Claro, que son las existentes actualmente en Ecuador. Para la recepción de llamadas se seleccionó un chip de cada operadora, permitiendo de esta forma usar el servicio de datos de cada una de ellas.

- **Movistar.**

  Con esta operadora se programó al generador para que realice un total de 300 llamadas, de las cuales 256 son las recibidas, significando una eficiencia de 85.33%. Ver tabla 16.

Tabla 16:

Llamadas Movistar.

Tipo de llamadas	Cantidad
Generadas	300
Recibidas	256
No Completadas	44
Eficiencia	85.33%

La visualización de la tabla 17 evidencia que de las 256 llamadas recibidas, 18 ingresaron a través del aplicativo Viber.

Tabla 17:

Llamadas Completadas Movistar.

Llamadas Completadas	Cantidad
Red conmutada CNT	256
Viber	18

- **Claro**

  La programación del generador fue de 500 llamadas con esta operadora, donde las recibidas se posicionaron con un número de 463 y una eficiencia del 87.66%. Ver tabla 18.

Tabla 18:

Llamadas Claro.

Tipo de llamadas	Cantidad
Generadas	300
Recibidas	263
No Completadas	37
Eficiencia	87.66%

De las llamadas recibidas, no hubo registro de ingresadas a través de Viber, posiblemente por el corto período en el que se llevó a cabo estas pruebas. Ver tabla 19.

Tabla 19:

Llamadas Completadas Claro.

Llamadas Completadas	Cantidad
Red conmutada CNT	263
Viber	0

4.3.2.3 Pruebas de conexión WiFi.

Se usó a Netlife, TVCable y a la Corporación Nacional de Telecomunicaciones CNT como proveedores del servicio de Internet, y se trasladó el receptor de llamadas a diferentes locaciones. El proceso realizado consistió en la desactivación del servicio de datos o de acceso a Internet a través de la operadora para la posterior conexión del receptor de llamadas a la red WiFi correspondiente a cada empresa proveedora.

- **CNT:** Las pruebas se realizaron en el laboratorio de pruebas del área de Prevención de Fraude de la Corporación Nacional de Telecomunicaciones CNT EP. La programación del generador fue para un total de 2800 llamadas, de las cuales 2634 fueron las recibidas, posicionándose con un 94,07% de eficiencia. Ver tabla 20.

Tabla 20:

Llamadas CNT.

Tipo de llamadas	Cantidad
Generadas	2800
Recibidas	2634
No Completadas	166
Eficiencia	94.07%

Al llevar a cabo estas pruebas no hubo resultados positivos en cuanto a regis-

tro de llamadas recibidas ingresadas por el aplicativo Viber. Ver tabla 21.

Tabla 21:

Llamadas Completadas CNT.

Llamadas Completadas	Cantidad
Red conmutada CNT	2634
Viber	0

- **TvCable:** Las pruebas con este proveedor se realizaron en el domicilio del señor Andrés Cabrera, ubicado en las calles Río Coca y 6 de Diciembre de la ciudad de Quito, provincia de Pichincha. .

  En las pruebas con este proveedor, cuyos resultados son visibles en la tabla 22, se programó al generador para que realice un total de 500 llamadas, de las cuales son 215 las recibidas, constituyendo una eficiencia de 42.6%, valor bajo debido a que se presentó un inconveniente de intermitencia en el servicio de telefonía móvil, el cual no permitió que las llamadas se completen.

Tabla 22:

Llamadas Tv Cable.

Tipo de llamadas	Cantidad
Generadas	500
Recibidas	213
No Completadas	287
Eficiencia	42.6%

En la tabla 23 se visualiza que las 213 llamadas recibidas ingresaron por la red conmutada CNT, y ninguna a través del aplicativo Viber.

Tabla 23:

Llamadas Completadas Tv Cable.

Llamadas Completadas	Cantidad
Red conmutada CNT	213
Viber	0

- **Netlife:** La locación para las pruebas con este proveedor fue el domicilio del Dr. Santiago Lemos, ubicado en Conocoto, cantón Rumiñahui de la provincia de Pichincha.

  Se programó al generador para que realice un total de 500 llamadas, de las cuales las recibidas fueron 485, significando una eficiencia de 97%. Ver tabla 24.

Tabla 24:

Llamadas Netlife.

Tipo de llamadas	Cantidad
Generadas	500
Recibidas	485
No Completadas	15
Eficiencia	97%

Con el proveedor Netlife, al igual que con TvCable, no ingresaron llamadas a través del aplicativo Viber. Ver tabla 25.

Tabla 25:

Llamadas Completadas NetLife.

Llamadas Completadas	Cantidad
Red conmutada CNT	485
Viber	0

4.4 Análisis de Resultados

Durante el lapso en el cual se llevaron a cabo las pruebas se pudo contabilizar un total de 12491 llamadas generadas, de las cuales 9065 son las recibidas exitosamente en los distintos escenarios. Las principales causas que justifican la pérdida de 3426 llamadas se detallan a continuación:

- Falla de conexión con la operadora prestadora de servicio de llamadas internacionales.
- Falla en terminación de llamada internacional por parte de la operadora de servicio de llamadas internacionales.
- Insuficiencia de saldo en las tarjetas.
- Cancelación o bloqueo de tarjetas por parte de la operadora de servicio de llamadas internacionales.

El tráfico ingresado por el aplicativo Viber, un total de 89 llamadas, tuvo registros hasta el mes de marzo de 2016; a partir de ese mes no se obtuvo resultados en cuestión de desvío de tráfico internacional entrante a través de este medio. Este aspecto influye en los resultados en las pruebas cuyos escenarios son el cambio de proveedor de red WiFi y el cambio de operador de telefonía móvil usando la banda 4G.

4.4.1 Pruebas a través de conexión SMA

Como se observa en la figura 20, los resultados de *ByPass* por medio de Viber alcanzan valores significativos en la red 4G con un 2.8% de incidencia sobre el total de llamadas entrantes, no así el caso de las redes 2G y 3G que presentan valores mínimos, condición dada probablemente porque Viber comprueba un estado de conexión óptima para garantizar calidad de servicio en la llamada.

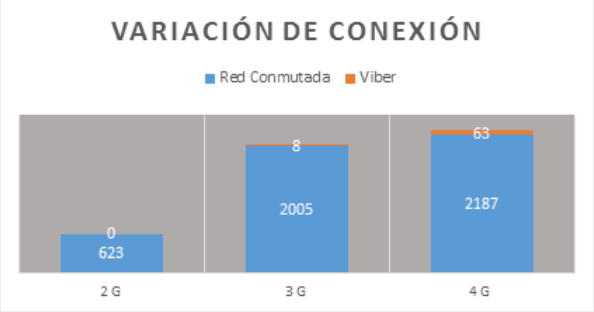


Figura 20: Variación de Conexión.

4.4.2 Pruebas de conexión WiFi

En este escenario y para los tres proveedores de internet, no se registró ninguna llamada entrante por el aplicativo Viber, ya que estas pruebas se realizaron en el mes de mayo y se debe considerar que desde marzo, no hubo registros de ingreso de llamadas por el aplicativo.

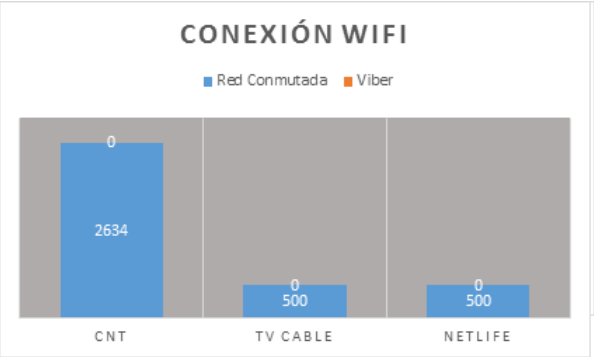


Figura 21: Variación de conexión Wifi.

4.4.3 Variación de Operadora

Las pruebas realizadas mediante las operadoras Movistar y Claro se realizaron en el mes de agosto 2016, y, a pesar de que desde marzo no se obtuvieron registros de tráfico entrante a través del aplicativo Viber, Movistar registró un 7,03% de llamadas ingresadas mediante este medio, esto por cuanto las pruebas realizadas con esta operadora se llevaron a cabo desde el mes de diciembre de 2015. Ver figura 22.

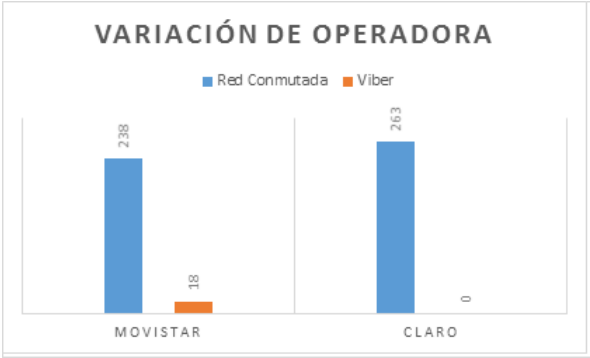


Figura 22: Variación de Operadora.

4.4.4 Resumen de resultados

Se presenta los cuadros resumen de los resultados separados por operador, uno que abarca todas las pruebas realizadas en los distintos escenarios para la Corporación Nacional de Telecomunicaciones CNT EP y uno que contiene los datos de las otras operadoras y resto de escenarios.

- **Pruebas CNT**

  Como se puede observar en la tabla 26 el mayor porcentaje de incidencia de llamadas internacionales entrantes por medio del aplicativo Viber fue en 4G con un 2.8% del total de las pruebas, seguido de 3G con un 0.34%. Estos resultados se registraron hasta el mes de marzo de 2016, las pruebas con WiFi se las realizó desde el mes de abril, lo cual pudo incidir en los resultados ya que desde marzo del 2016 no se registran eventos Viber.

Tabla 26:

Cuadro Pruebas CNT.

Escenario	Generadas	Red Normal	Viber	No completadas	Eficiencia	Viber
2G	1000	623	0	377	62.3%	0%
3G	2500	2005	8	397	84.12%	0.34%
4G	3891	2187	63	1641	57.82%	2.8%
WiFi	2800	2634	0	166	94.07%	0%

- **Otros escenarios**

  Los resultados positivos en la operadora Movistar se dieron a partir del mes de diciembre de 2015, que fue cuando se iniciaron las pruebas. El resto de escenarios se evaluaron en los meses de Abril y Mayo de 2016.

Tabla 27:

Cuadro Pruebas Otros Escenarios.

Escenario	Generadas	Red Normal	Viber	No completadas	Eficiencia	Viber
Movistar	300	238	18	44	85.33%	7.03%
Claro	300	263	0	37	87.66%	0%
TvCable	500	213	0	287	42.6%	0%
Netlife	500	485	0	15	97%	0%

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se implementó una solución acorde a los requerimientos establecidos por la CNT que permite la generación automática de llamadas y la detección de ByPass tipo OTT a través el aplicativo Viber.

El desarrollo de la solución permitió demostrar la existencia del fraude OTT *ByPass* mediante Viber, este hecho es de profunda importancia para el entorno local ya que al ser un nuevo tipo de fraude es necesario definir estrategias de combate tanto por los operadores móviles como por el regulador.

El fraude *ByPass* evoluciona constantemente buscando encontrar nuevas rutas grises que permitan la terminación no autorizada de tráfico telefónico internacional. La aplicación desarrollada es un paso importante dado por CNT como pionero en la detección de este nuevo tipo de fraude en Ecuador y probablemente en Latinoamérica.

Se demostró que el fraude OTT *ByPass* es una realidad que está afectando a los operadores CNT y Movistar. Debido a la poca cantidad de pruebas realizadas al ope-

rador Claro no fue posible detectar casos positivos, sin embargo, dada la cuota de mercado que maneja este operador existe una alta probabilidad que este escenario también este generando pérdidas en su red.

El aplicativo al ser desarrollado en un sistema operativo móvil como lo es Android, permite que su ejecución se realice en terminales de bajo costo y alto desempeño permitiendo así conformar un escenario completo de pruebas en donde se encuentren tres o cuatro sistemas implementados, ahorrando una cantidad considerable en infraestructura e implementación.

La implementación de la solución dentro de un teléfono móvil permite dotar al sistema de movilidad sin involucrar costo de transporte o incomodidad al técnico de prueba, es así como se aportó portabilidad al sistema de llamadas de lazo, permitiendo no solo enfocarlo en la generación de llamadas para la detección de OTT *Bypass*, sino que con unos pequeños cambios pueda funcionar como robot para detección de otro tipo de *Bypass* generado por la telefonía móvil o aplicaciones OTT.

El desarrollo de los teléfonos inteligentes así como el mejoramiento de sus sistemas operativos ha dado lugar a que las nuevas versiones sean las más populares en el mercado siendo así que el sistema se empezó programándolo con una base de Android 2.3 con la finalidad de alcanzar una cobertura total dentro de los teléfonos inteligentes, pero al momento de su culminación era necesario usar teléfonos que permitan una conexión 4G, los cuales vienen con software predeterminado Android 4.1 con el cual función perfectamente el sistema y se dio cobertura al 95.2% de teléfonos inteligentes existentes en el mercado.

Viber es un aplicativo OTT con prestación de servicios de mensajería y telefonía IP de forma gratuita todo esto mediante el uso de la red móvil o internet, la diferencia con otros aplicativos es la calidad en cuestión de prestación de servicios de voz, esto se pudo comprobar con las pruebas en los distintos anchos de banda, dando como resultados una mayor incidencia de terminación de llamadas por este medio cuando el

ancho de banda era el óptimo para que una llamada sea exitosa en cuanto a conexión, es decir con redes WiFi con buen ancho de banda, y redes móviles 3G y 4G.

La generación de llamadas implementada como parte del sistema, permite que el técnico o usuario del sistema configure una sola vez al día el sistema, o en caso de los fines de semana permita que el sistema funcione automáticamente sin necesidad de una constante revisión o manipulación, permitiendo así que el sistema se acerque lo más posible a un sistema autónomo.

Al poder ingresar las tarjetas tanto desde el teléfono como desde la aplicación Web brinda al usuario comodidad y portabilidad al momento de hacer un cambio o una ejecución con una tarjeta nueva o con una ya existente, pero con un nuevo PIN, pudiendo así el usuario del sistema realizar pruebas desde cualquier parte del mundo y hacia cualquier destino.

El sistema Web permite al usuario monitorear eventos pasados, ingresar o modificar los datos de las tarjetas sin necesidad de que el sistema se encuentre en la misma locación, basta con tener acceso desde un computador al internet, y tener el usuario y la clave correctas para acceder al sistema y obtener toda la información que este brinda.

El algoritmo para la generación del lazo de llamadas fue diseñado de tal forma que la ejecución del aplicativo no dependa de la terminación o la realización de una llamada en forma exitosa, en caso de que el usuario corte la llamada, o la llamada sea interrumpida antes de cumplir la ejecución completa el sistema seguirá con su contador intacto, y ejecutará una nueva secuencia cuando el tiempo sea el correcto.

El usuario al tener el control de que tarjetas usar y la cantidad de llamadas que generar, le da al sistema capacidad de adaptabilidad de acuerdo a la necesidad del usuario, el mismo que escogerá si usa desde una o hasta cuatro tarjetas para las pruebas y también el tiempo en que se encontrará ejecutándose.

La tabulación de las pruebas debe ser diaria para facilitar la detección de un evento Viber, puesto que el aplicativo Viber viene programado por defecto para emitir en su registro solo un evento por día de un mismo número o usuario. Haciendo que si en dos días se registró dos o más eventos por el mismo número de origen solo se guarde el último, lo que afectaría para la contabilización correcta y la emisión de un informe con información exacta.

La Corporación Nacional de Telecomunicaciones CNT EP, cuenta con un amplio desarrollo en cuanto a sistemas de detección y prevención de fraude en el ámbito de las telecomunicaciones, actualmente se encuentra concentrado y orientado en la detección de Fraude por medio de la telefonía móvil siendo así que se tiene implementado un sistema de llamadas de lazo automático, el mismo que sirvió de base fundamental para el desarrollo del sistema descrito en este trabajo.

5.2 Recomendaciones

Se recomienda realizar un análisis del tráfico LDI entrante, para determinar los países con mayor incidencia o número de llamadas generadas hacia nuestro país con el fin de delimitar los posibles escenarios de potencial fraude.

Se recomienda que antes de usar el sistema se compruebe la conexión a internet o acceso al servidor, ya que sino la ejecución se verá afectada y no funcionará el sistema correctamente puesto que nos datos necesarios para la llamada se encuentran en el servidor.

Así mismo comprobar la cobertura y la calidad de la señal de la telefonía móvil, ya que si el sistema se encuentra ubicado dentro de una zona en donde la calidad de señal no sea buena es muy posible que le ejecución de las llamadas no se completen exitosamente. Tener siempre a los teléfonos con un buen porcentaje de batería al inicio

de cada ejecución de pruebas, dado que como el sistema funciona continuamente tanto el receptor como el generador consumirán la batería mucho más rápida que cuando se encuentra el teléfono en un normal desempeño.

En caso de tener el número de llamadas generadas muy superior a las llamadas recibidas, verificar el saldo de las tarjetas ingresadas en el sistema, dado que hay tarjetas que tienen tiempo de caducidad desde su primera llamada.

Se recomienda como trabajo futuro mejorar el aplicativo en parámetros de extracción y tabulación de llamadas entrantes y salientes del teléfono, así como la extracción automática de los registros del aplicativo Viber para permitir al sistema ser completamente autónomo.

En caso de que el usuario por accidente corte la llamada que estaba en ejecución en ese momento no se debe volver a iniciar la ejecución del sistema, ya que solo esa prueba no se completará, pero el sistema continuara con el correcto funcionamiento luego de la espera del tiempo programado.

Rotar cada cierto tiempo los chips de los teléfonos tanto del generador como del receptor, así como los pines de las tarjetas que se están usado, esto con la finalidad de una mejor ejecución del sistema y un mejor escenario de prueba, porque el *carrier* identificar que se realizan llamadas de lazo por el mismo número telefónico y mismo pin de tarjeta prepago y puede tomar una medida para que todo el trafico con esos datos sea enviado por la ruta normal.

Se recomienda que se lo use al teléfono con un solo método de conexión ya sea la red WiFi o Datos móviles, no dejando a que el teléfono pueda escoger analizando el ancho de banda o la calidad de la red ya que puede coincidir en un momento de intercambio de conexión el sistema falle y se altere la ejecución del mismo.

Se recomienda utilizar la solución con el fin de realizar un estudio económico de

las potenciales pérdidas económicas causadas al operador con base en los minutos que estarían siendo terminados en Viber en lugar de la red del operador.

BIBLIOGRAFÍA

Android. (2015). *The android source code.* Recuperado de: https://source.android.com/source/index.html.

Android. (2016a). *Api version distribution.* Recuperado de: https://developer.android.com/about/versions/android-4.1.html.

Android. (2016b). *Conoce android studio.* Recuperado de: https://developer.android.com/studio/intro/index.html.

Arraxe. (s.f). *Desvio ott.* Recuperado de: http://www.araxxe.com/desvio-de-ott.html.

Barreno, D., Carrión, D., & Mejía, I. (2016). Evolución de la tecnología móvil. camino a 5g. *Contribuciones a las Ciencias Sociales*.

Castillo, A. (2015). *Diseño e implementación de un sistema de gestión automática para vehículos sobre la plataformaANDROID.* (Unpublished doctoral dissertation).

Castillo, F. (2015). Ott bypass. *Telefónica*.

Cevallos, D., & Ortiz, R. (2016). *Análisis del rendimiento de transmisión de datos en redes móviles (2G, 3G, 4G) para diferentes configuraciones de la pila TCP-IP.* (Unpublished doctoral dissertation).

de Telecomunicaciones y Sociedad de la Información, M. (2016). *Mejores servicios para los ecuatorianos gracias al trabajo realizado por arcotel.* Recuperado de: http://www.telecomunicaciones.gob.ec/mejores-servicios-para-los-ecuatorianos-gracias-al-trabajo-realizado-por-arcotel/.

Developer, A. (2016). *Api version distribution.* Recuperado de: https://developer.android.com/about/versions/jelly-bean.htm.

Gonzáles, T. (2012). *Las 5 mejores versiones de android os.* Recuperado de: http://computerhoy.com/listas/moviles/5-mejores-versiones-android-os-1706.

Meza, M. (2007). *Fraudes en telecomunicaciones* (Vol. 1). Publiasesores.

Orquera, E. (2014). *Análisis de protocolos de señalización para la detección de comportamientos irregulares en las líneas de telefonía fija, en el softswitch de Quito perteneciente a la CNT EP, utilizando sondas de señalización* (Unpublished doctoral dissertation).

Potro, J., & Maria, M. (2013). *Definición de Fraude.* Recuperado de: http://definicion.de/fraude/.

Raya, A. (2011). *Android 4.0 ice cream sandwich es oficial, así es su interfaz de usuario.* Recuperado de: http://www.xatakamovil.com/sistemas-operativos/android-40-ice-cream-sandwich-es-oficial-asi-es-su-interfaz-de-usuario.

Singarayar, S. (2016). *Ott.* Recuperado de: http://analogypartners.com/ott/.

s.n. (2014). *Going ott.* Recuperado de: http://www.dotecon.com/publications/going-ott/.

Solis, F., & Vaca, X. (2014). *Evaluación del sistema de telefonía IP Asterisk mediante la implementación de un prototipo de red en ambientes IPv4 e IPv6* (Unpublished doctoral dissertation).

TICbeat. (2010). *Características de android 2.3 gingerbread.* Recuperado de: http://www.ticbeat.com/sim/caracteristicas-android-23-gingerbread/.

TICbeat, R. (2010). *Funciones de android 2.3 para desarrolladores.* Recuperado de: http://www.ticbeat.com/sim/funciones-android-2-3-desarrolladores/.

Universo, E. (2015). *Con mÃ¡s espacios en las bandas para 4g.* Recuperado de: http://www.eluniverso.com/noticias/2015/02/26/nota/4592656/mas-espacios-bandas-4g.

Viber. (2016a). *Preguntas frecuentes.* Recuperado de: https://www.viber.com/es/faq.

Viber. (2016b). *Viber for android.* Recuperado de: https://www.viber.com/es/products/android.