ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO DE UN SISTEMA DE DETECCIÓN Y CONTROL DEL FRAUDE EN LA PRESTACIÓN DE LOS SERVICIOS DE TELEFONÍA FIJA Y SERVICIO MÓVIL AVANZADO EN EL ECUADOR”

INFORME DE MATERIA INTEGRADORA

Previa a la obtención del Título de:

INGENIERA EN ELECTRÓNICA Y TELECOMUNICACIONES

CAMACHO SELLÁN KATHERINE MICHELLE

GONZÁLEZ MORA MARÍA GABRIELA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTOS

A lo largo de nuestro caminar, ha sido Dios quien nos ha sostenido, guiado y ayudado a seguir corriendo hasta esta meta, primeramente a Él sea toda la Gloria, el honor y la alabanza por todos los logros obtenidos en esta etapa.

Agradecemos con gran regocijo a nuestros Padres y familia, quienes han sido nuestros pilares fundamentales, ellos nos han alentado y animado en tiempos de dificultad, con su sabiduría nos han encaminado y exhortado para terminar lo que en el 2010 empezamos, nos han desafiado a dar lo mejor de nosotros pese a las circunstancias, ellos han sido quienes ven nuestras debilidades, pero nos impulsan a convertirlas en oportunidades para seguir creciendo; agradecemos a estos seres maravillosos que Dios nos regaló como nuestra familia.

La paciencia para enseñarnos, la bondad para compartir sus conocimientos y el tiempo que nos han dedicado para resolver nuestras dudas, son algunos de los regalos que los maestros nos han dado; gracias a todos nuestros profesores por creer en nuestra generación, por su preocupación para darnos una enseñanza de calidad y formarnos como profesionales integrales, gracias por su humildad y valor para corregirnos y alentarnos a desarrollar nuestras habilidades. Gracias al tutor de este proyecto integrador, PhD. Freddy Villao, por su tiempo, paciencia, guía y enseñanza a lo largo de este difícil periodo de investigación y desarrollo.

Un camino se vuelve más placentero cuando se lo recorre con amigos, gracias a nuestros compañeros de batallas, con quienes hemos compartido conocimientos, experiencias, alegrías, tristezas, victorias y fracasos. Ellos han sido quienes desde la cancha nos han alentado a continuar, quienes en medio de tropiezos nos han tendido la mano para juntos avanzar y quienes con sus bromas y ocurrencias han hecho que nuestro transitar sea más divertido.

Un especial agradecimiento a nuestra universidad, la cual abre sus puertas a jóvenes como nosotras para prepararnos en ciencia, liderazgo y responsabilidad social. Gracias ESPOL porque es un orgullo pertenecer a esta institución y siempre nos sentiremos honradas de ser llamadas politécnicas.

Las Autoras

DEDICATORIA

Este proyecto y todo el esfuerzo plasmado en cada página lo dedicamos a nuestros padres:

Sra. Sarita Sellán Medina

Sra. María Mora

Sr. Freddy Camacho Zavala

Sr. Gustavo González Ramón

Quienes han sido partícipes de la dedicación necesaria para su desarrollo y quienes con su ejemplo nos han animado a seguir adelante.

A nuestros hermanos, familiares y amigos que nos ayudaron a mantenernos enfocadas y muchas veces tomaron parte de nuestras responsabilidades para que nosotras pudiéramos realizar las actividades investigativas que este proyecto demandó.

A las generaciones futuras de estudiantes politécnicos y de ingenieros electrónicos y de telecomunicaciones para que se esfuercen por alcanzar sus objetivos y sean partícipes de actividades investigativas con el fin de servir a la sociedad y mejorar la calidad de vida de todos los ecuatorianos y humanos en general.

A los jóvenes de nuestro país, quienes tienen la responsabilidad de prepararse eficientemente para enfrentar las dificultades y problemas que aquejan cada sector; les dedicamos este proyecto para impulsarlos a utilizar bien sus conocimientos, a fin de ser aprovechados para beneficio de todos.

Las Autoras

TRIBUNAL DE EVALUACIÓN

Dr. Freddy Villao Quezada, PhD.	**Ing. José Menéndez Sánchez, MSc.**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Katherine Michelle Camacho Sellán

María Gabriela González Mora

RESUMEN

La necesidad de comunicación ha originado la creación de diversos tipos de fraudes en el sector de las telecomunicaciones; estos delitos representan un problema a nivel mundial, pues cada vez son más las medidas internacionales que se han tomado para revertir los efectos económicos que ocasionan en todo el mundo.

En los últimos años el fraude producido a las diferentes prestadoras de servicio de telefonía fija y servicio móvil avanzado en el Ecuador ha dejado de ser empírico o básico, pues el avance de la tecnología ha ocasionado que los estafadores empleen mejores técnicas y creen nuevos delitos que burlan las estrategias antifraude instauradas por las prestadoras de servicios de telecomunicaciones.

En el Ecuador se están desarrollando nuevas modalidades de fraude, pero no se han tomado las medidas necesarias para controlarlas, este hecho provocará el aumento de las posibilidades y frecuencia con que se cometen estos delitos, que podría generar un gran perjuicio tanto a operadoras, usuarios y al Estado, en el futuro inmediato.

Los sistemas empleados actualmente por las empresas de telecomunicaciones no pueden detectar los fraudes por OTT (Over the Top) ni Bypass desde smartphone, por lo cual este proyecto integrador aporta con el diseño de dos sistemas basados en la metodología del loop de llamadas, complementando así las actuales estructuras antifraude que tienen las operadoras, para lograr la detección oportuna de estas dos nuevas tendencias de fraude.

Cada sistema propuesto brinda la facilidad de ajustarse a los recursos técnicos que poseen las empresas, sin necesidad de migrar la tecnología o de adquirir nuevos equipos costosos para su implementación.

Como resultado de la detección eficiente se evitará pérdidas considerables de dinero para las operadoras y el Estado; mejorando de esta manera la economía del país y situando al Ecuador como un ejemplo de los países que previenen eficientemente el fraude producido en la telefonía fija y móvil.

ÍNDICE GENERAL

AGRADECIMIENTOS ii

DEDICATORIA iii

TRIBUNAL DE EVALUACIÓN iv

DECLARACIÓN EXPRESA v

RESUMEN vi

ÍNDICE GENERAL vii

CAPÍTULO 1 1

1. EL FRAUDE EN LA PRESTACIÓN DE LOS SERVICIOS DE TELEFONÍA FIJA Y MÓVIL EN EL ECUADOR 1

1.1. El Fraude en Telecomunicaciones en el Mundo 1

1.2. Estadísticas del servicio de telefonía fija y servicios móviles avanzados en el Ecuador 4

1.3. Evolución del Fraude en el sector de las telecomunicaciones en el Ecuador 5

1.4. Actuales tendencias de Fraude en el Ecuador 7

1.4.1. Fraude por Bypass 7

1.4.2. Clonación de celulares 16

1.4.3. Fraude de Tercer País 19

1.4.4. Hackeo de centrales PBX 20

1.4.5. Refilling 23

1.4.6. Fraude por roaming 24

1.4.7. Falsa Respuesta a llamada 25

1.4.8. Fraude por OTT 27

1.4.9. Fraude de Suscripción.....30
1.4.10. Fraude Interno.....31
1.5. Impacto del Fraude en telefonía fija y móvil.....32
1.6. Objetivos.....34
1.6.1. Objetivo General.....34
1.6.2. Objetivos específicos.....35
1.7. Justificación.....35
1.8. Alcance del proyecto integrador.....36
CAPÍTULO 2.....37
2. SISTEMAS DE DETECCIÓN Y CONTROL DEL FRAUDE EN SERVICIOS DE TELEFONÍA FIJA Y MÓVIL.....37
2.1. Criterios de Detección y Estrategias de Prevención por tipo de fraude.....38
2.1.1. Bypass.....38
2.1.2. Clonación de celulares.....39
2.1.3. Fraude de tercer país.....39
2.1.4. Hackeo PBX en Ecuador.....40
2.1.5. Refilling.....43
2.1.6. Fraude de roaming.....43
2.1.7. Falsa respuesta a llamada.....44
2.1.8. Fraude de suscripción.....44
2.1.9. Fraude interno.....45
2.2. Sistemas de detección de fraude utilizados en el Ecuador.....46
2.2.1. Loop de Llamadas (Lazos Telefónicos de llamadas).....47

2.2.2. Análisis de CDRs Internacionales....50
2.2.3. Perfilamiento....53
2.3. Diseño de sistema para la Detección de Fraude en telefonía fija y móvil en Ecuador....55
2.3.1. Sistema de detección de fraude Bypass producido desde smartphones....56
2.3.2. Fraude OTT....61
CAPÍTULO 3....70
3. RESULTADOS Y BENEFICIOS....70
3.1. Resultados....70
3.1.1. Análisis económico de la implementación....70
3.2. Beneficios....72
3.2.1. Beneficio de la técnica de detección utilizada....73
3.2.2. Factibilidad de la implementación....73
3.2.3. Escalabilidad....74
3.2.4. Plataforma anti Baneo....74
3.2.5. Beneficios para la operadora, usuarios y Estado ecuatoriano....75
CONCLUSIONES Y RECOMENDACIONES....77
Conclusiones....77
Recomendaciones....78
BIBLIOGRAFÍA....79
ANEXO A: ÍNDICE DE ABREVIATURAS....84
ANEXO B: ÍNDICE DE FIGURAS....86
ANEXO C: ÍNDICE DE TABLAS....88

CAPÍTULO 1

1. EL FRAUDE EN LA PRESTACIÓN DE LOS SERVICIOS DE TELEFONÍA FIJA Y MÓVIL EN EL ECUADOR

Desde que la telefonía apareció, ha llegado a convertirse en un factor muy importante para el progreso del mundo que hoy conocemos, con el paso del tiempo, la telefonía ha ido evolucionando y con ella también el desarrollo de nuevas técnicas y modelos para cubrir las continuas demandas de los usuarios y sociedad en general.

1.1. El Fraude en Telecomunicaciones en el Mundo

La UIT (Unión Internacional de Telecomunicaciones), mediante datos estadísticos, muestra la densidad de los servicios de telefonía fija y móvil por cada 100 habitantes (Figura 1.1). En el presente año, la telefonía móvil presenta un significativo crecimiento de 37,1% más con respecto al año 2008, mientras que la telefonía fija aún está presente con el 14,5% [1].

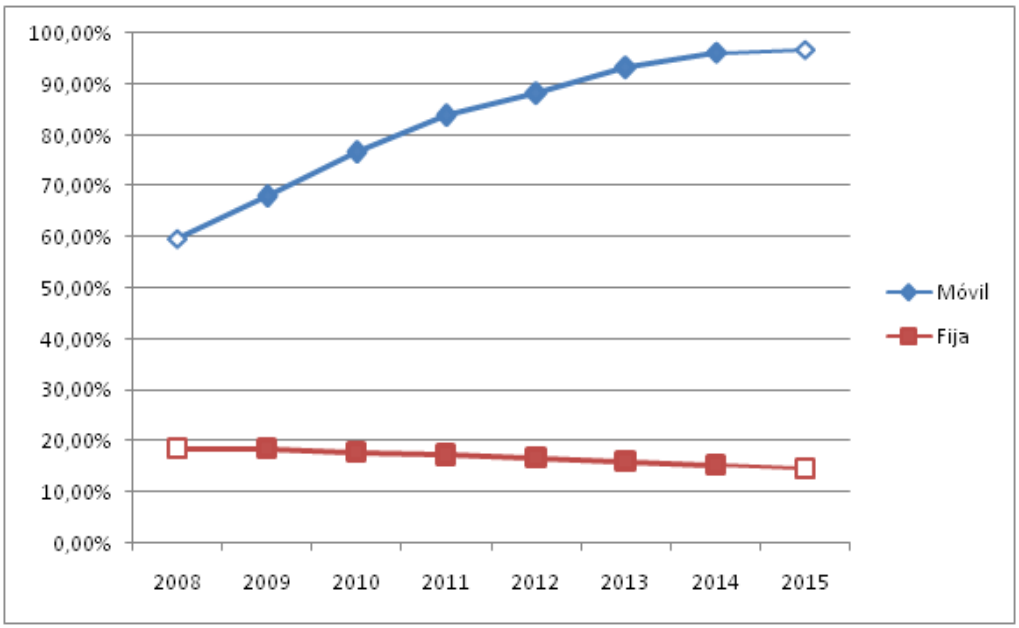


Figura 1.1: Evolución de la telefonía fija y móvil en el mundo (por cada 100 habitantes) [1].

La necesidad de comunicación y la constante evolución tecnológica, ha originado la creación de diversos tipos de fraudes en el sector de las telecomunicaciones; estos delitos representan un problema a nivel mundial, pues cada vez son más las medidas internacionales que se han tomado para revertir los efectos económicos que ocasionan en las operadoras de telefonía fija y móvil en todo el mundo.

El Diario ABC de España reporta que “Un grupo de «piratas» se encarga de hackear el software de la centralita telefónica de una pequeña empresa para hacer un sinfín de llamadas «gratis». Es una estafa difícil de detectar para los propietarios de las centralitas, porque suele ocurrir en las noches.” [2].

En el sector de las telecomunicaciones, mundialmente, existen agentes que buscan desarrollar actividades que les permitan obtener un lucro económico indebido, adoptando diversas técnicas que evolucionan con el tiempo. “La lucha contra el fraude en la telefonía móvil y las diferentes medidas para combatir el robo de terminales son desafíos fundamentales para las operadoras de la región que deben encarar de forma conjunta” [3], aseguró Diego Bassanelli, Gerente de Fraude de Telecom Personal Argentina.

En la Figura 1.2 se presentan los fraudes que mayores pérdidas han ocasionado, según el análisis anual que realiza la CFCA (Communications Fraud Control Association), en el sector de las telecomunicaciones a nivel mundial [4].

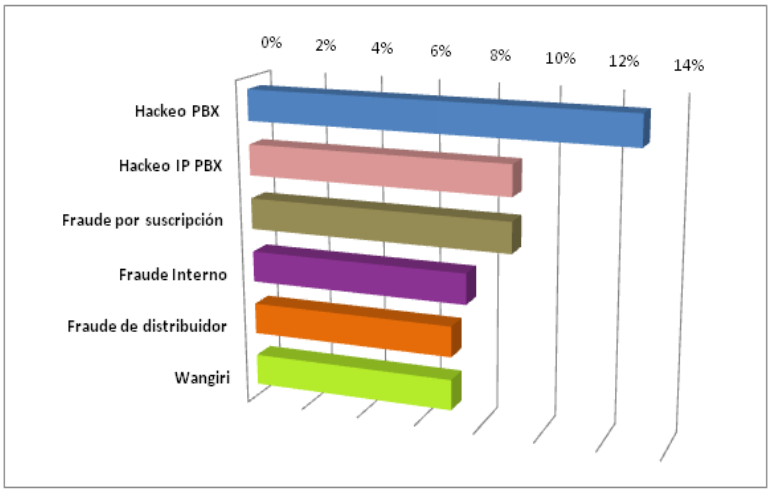


Figura 1.2: Métodos de Fraudes en telecomunicaciones más comunes en el mundo (2015).

Los fraudes más comunes generan notables pérdidas a nivel mundial, sin embargo éstos no son los únicos que se practican actualmente. Existen diversos tipos de fraude que, a pesar de no ser ejecutados con frecuencia, ocasionan pérdidas a las diferentes prestadoras de servicio de telefonía fija y móvil; vale recalcar que por mínimas que sean, éstas terminan perjudicando a la economía mundial de manera significativa.

Las pérdidas estimadas en billones de dólares debido al fraude en telefonía fija y móvil a nivel mundial pueden ser observadas en la Figura 1.3.

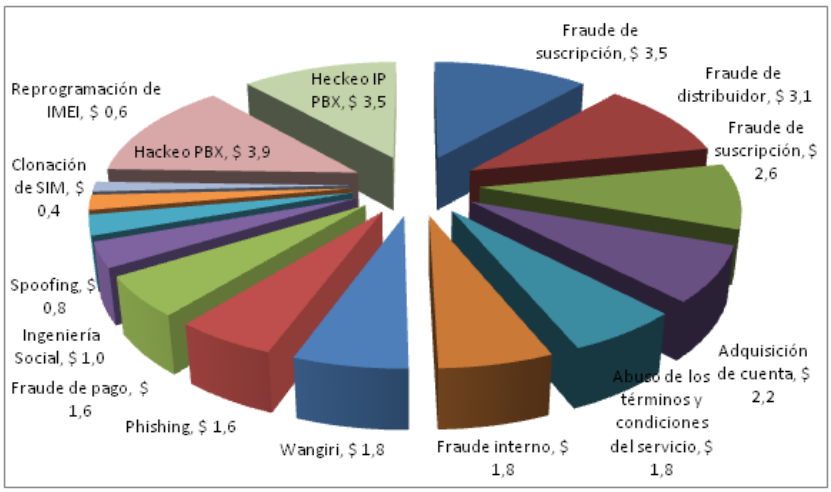


Figura 1.3: Pérdidas estimadas en Billones de dólares por método de fraude (2015) [4].

1.2. Estadísticas del servicio de telefonía fija y servicios móviles avanzados en el Ecuador

La telefonía fija y móvil representan los servicios de telecomunicaciones que mayores ingresos producen en el Ecuador, consolidándose como uno de los negocios más rentables [5].

En la actualidad, 6 empresas se encuentran prestando servicios de telefonía fija; la concesión a nivel nacional es de la Corporación Nacional de Telecomunicaciones CNT EP y las otras 5 empresas concentran su operación en los sectores detallados en la Tabla 1 [6].

OPERADORA	ÁREA DE OPERACIÓN ACTUAL
CNT EP	A nivel nacional
ETAPA EP	Azuay, Guayas, Pichincha y El Oro
LINKOTEL S.A.	Guayas y Manta
SETEL S.A.	Guayas, Pichincha, El Oro, Manabí, Tungurahua con Servicio de Abonados y Telefonía Pública; Chimborazo, Imbabura y Santo Domingo de Los Tsáchilas con Servicio de Telefonía Pública.
ECUADORTELECOM S.A. (Claro Fijo)	Guayas, Pichincha, El Oro, Manabí e Imbabura
LEVEL 3 ECUADOR LVLT S.A.	Quito, Valles de Los Chillos y Tumbaco

Tabla 1: Operadoras de servicio de telefonía fija en el país [6]

El Servicio Móvil Avanzado es prestado por CONECEL S.A. (Claro), OTECEL S.A. (Movistar) y CNT EP (Corporación Nacional de Telecomunicaciones); siendo estas 3 empresas las únicas autorizadas para operar en el país [6].

Actualmente, existen 2.518.357 abonados en telefonía fija y 14.366.993 abonados en telefonía móvil, según datos estadísticos de la ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) [7] [8].

Cada operadora telefónica, tanto fija como móvil, poseen planes de expansión y buscan incrementar el número de abonados que poseen, por lo que invierten en recursos para mejorar la calidad del servicio y en estrategias de marketing para lograr sus objetivos [9], sin embargo el fraude en el sector de las telecomunicaciones produce perjuicios económicos significativos, no solo a las operadoras, sino también al Estado ecuatoriano y a los usuarios, generando la necesidad de que los medios de detección y control de fraude avancen a la par con las nuevas tecnologías y prácticas tecnificadas de los procedimientos ilícitos.

1.3. Evolución del Fraude en el sector de las telecomunicaciones en el Ecuador

En conjunto con el progreso tecnológico, las intenciones de aprovecharse de las vulnerabilidades de los sistemas de telecomunicaciones han ido evolucionando, desde las estafas de antaño, cuando a las monedas utilizadas en las cabinas telefónicas se les ataba un delgado hilo para luego recuperarlas**,** hasta la implementación de técnicas avanzadas que pretenden burlar los sistemas de autenticación y detección de las operadoras [10]. El desarrollo de estos ilícitos durante los primeros años se presenta en la Figura 1.4.

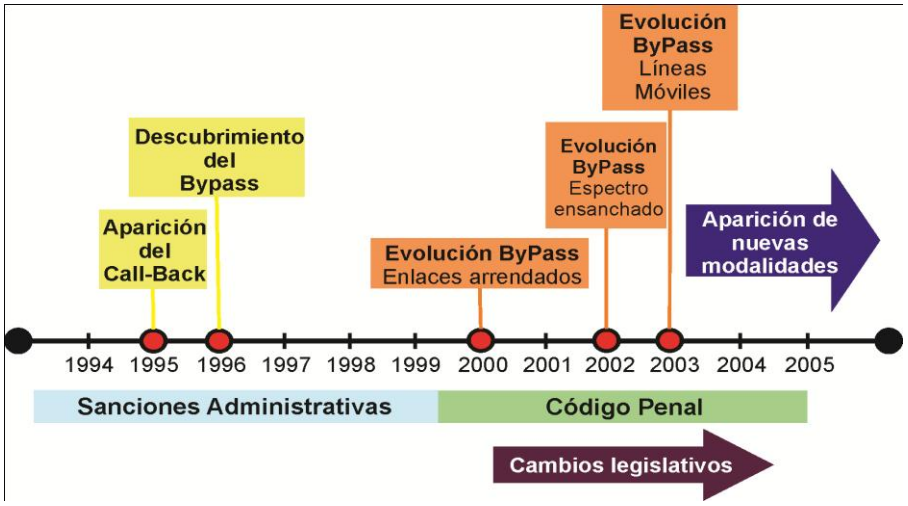


Figura 1.4: Evolución del fraude en telefonía

En 1995 se detecta el “Call Back” como primer tipo de fraude en el país, este permite efectuar llamadas internacionales salientes que luego se convierten en llamadas entrantes a la red nacional, para así evitar que la operadora facture por el servicio y beneficiarse de las bajas tarifas de las llamadas en el exterior. Este sistema también puede ser usado en llamadas nacionales [11].

Un año más tarde, en 1996 se descubre el fraude por Bypass que constituye una vía alterna al tráfico telefónico internacional para ser cobrado por la operadora como local, este sistema es el que mayor afectación económica ha causado en el país [11]. El fraude fue sancionado por la ex SUPERTEL (Superintendencia de Telecomunicaciones) de acuerdo a la ley vigente en ese entonces, para el 12 de agosto de 1999 el Artículo 422 del Código Penal fue modificado para señalar como delito los fraudes cometidos en el sector de las telecomunicaciones [12].

Durante la primera etapa de la evolución del sistema “Bypass” (1999-2000), la detección del mismo era posible porque quienes lo practicaban requerían de antenas parabólicas de grandes magnitudes y hacer uso de múltiples líneas telefónicas instaladas en un mismo lugar con tráfico internacional poco convencional [12].

Para dificultar la detección e intervención, desde el año 2000, los sistemas Bypass no emplean antenas fácilmente visibles y de complicado desmontaje,

pues ahora cuentan con un enlace internacional arrendado; hasta el 2002, para encubrir el fraude debían manipular físicamente las líneas telefónicas, adquiridas con documentaciones falsas y distribuidas en varios sectores, para luego instalarlas en un sitio clandestino común. Los sistemas de detección requirieron de una adaptación más técnica que permitiera identificar las líneas ilícitas en tiempo real [12].

A partir del año 2002, la tecnología del “espectro ensanchado” fue usada para cometer el fraude estableciendo enlaces microondas con el telepuerto, de esta forma las líneas telefónicas ya no se concentraban en un mismo sitio. Luego se constató el uso de equipos gateways para procesar las señales telefónicas y llegar a manejar los parámetros de señalización de una red de telefonía [13].

En el año 2003 se descubre por primera vez el “Bypass” con líneas telefónicas móviles, este suceso marcó el comienzo de una nueva etapa de fraude en telecomunicaciones, donde se desarrollan novedosas alternativas que dificultan la detección y facilitan la comercialización para el beneficio ilícito de una o un grupo de personas [12].

1.4. Actuales tendencias de Fraude en el Ecuador

En los últimos años el fraude ocasionado a las diferentes prestadoras de servicio de telefonía fija y servicio móvil avanzado en el Ecuador ha dejado de ser empírico o básico, pues el avance de la tecnología ha ocasionado que los estafadores empleen mejores técnicas y creen nuevos delitos que burlan las estrategias antifraude instauradas por las prestadoras de servicios de telecomunicaciones en el Ecuador.

A continuación se detalla los principales delitos de fraude en telefonía que se cometen en nuestro país, y se describe su funcionamiento de acuerdo a las nuevas tecnologías empleadas para el cometimiento de los mismos [14]:

1.4.1. Fraude por Bypass

El Bypass es la cara del fraude de telecomunicaciones en el Ecuador; este delito ha ocasionado pérdidas cuantiosas tanto para las operadoras

como para el Estado ecuatoriano. Actualmente no es sorpresa encontrar publicaciones de periódicos locales relatando los allanamientos de inmuebles que funcionaban como centrales telefónicas clandestinas (Figura 1.5); ejemplos como lo reportado a continuación por el diario "Extra" de la ciudad de Guayaquil el 15 de diciembre de 2011 nos advierten que el Bypass es una práctica ilícita muy común por lo que resulta necesario reforzar las estrategias de detección para este tipo de delitos. "Una casa ubicada en el solar 5, de la manzana 941, de Samanes V, fue allanada por miembros del Grupo de Operaciones Especiales (GOE), Fiscalía, Superintendencia de Telecomunicaciones y la perjudicada Ecuadortelecom SA. Allí se descubrió que funcionaba una central telefónica clandestina...este fraude se lograba a través de una señal por Internet, que receptaba las llamadas internacionales y mediante un sistema de retroalimentación de centrales internas se cambiaba los datos para hacerlos pasar como llamadas locales. "En este proceso investigativo se halló doce líneas telefónicas empleadas para este ilícito. Esto estimaría una pérdida aproximada de 12.000 dólares, que afectan a la empresa Ecuadortelecom SA", acotó Narváez." [13].

Figura 1.5: Sistema Bypass detectado en un sector de la ciudad de Guayaquil. [15]

BYPASS INTERNACIONAL ENTRANTE

Este fraude dirige el tráfico internacional evitando los cargos que cobran los operadores autorizados para prestar el servicio de larga distancia internacional [16].

Es un procedimiento mediante el cual operadores no autorizados inyectan llamadas entrantes internacionales en la red de un operador legal como si fueran llamadas locales [16].

PROCEDIMIENTO PARA REALIZAR EL BYPASS INTERNACIONAL ENTRANTE

Para describir el procedimiento de Bypass internacional entrante, es necesario dividirlo en cuatro etapas (Figura 1.6): Acceso a usuarios, Red internacional, Enlace y Distribución de llamadas [16].

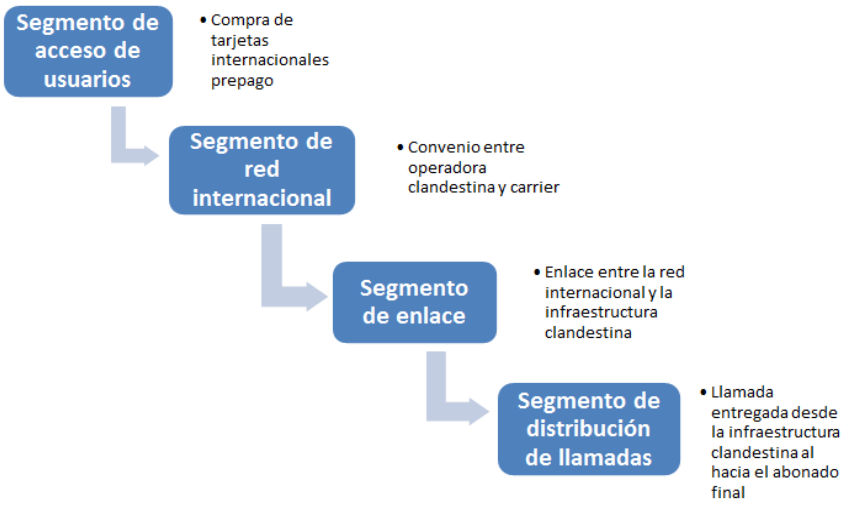


Figura 1.6: Etapas presentes en el Bypass internacional entrante [16].

SEGMENTO DE ACCESO A USUARIOS

En esta etapa, un usuario ubicado en el extranjero (Abonado A) que quiere realizar una llamada a Ecuador (Abonado B), le compra a un operador clandestino una tarjeta prepago (física o en línea) que permite realizar llamadas internacionales (Figura 1.7). Esta llamada puede ser realizada desde un teléfono público, fijo, móvil, softphones o portales IP [16].

Figura 1.7: Tarjetas prepago para llamadas internacionales [17]

Posteriormente, el usuario en el extranjero sigue los pasos indicados en la tarjeta y marca el número telefónico de Ecuador al cual desea llamar.

SEGMENTO DE RED INTERNACIONAL

Con el fin de enviar todas las llamadas originadas en la etapa anterior, el operador clandestino establece un convenio con una compañía portadora (carrier), la misma que dispone de la infraestructura y capacidad necesaria para transportar y terminar tráfico telefónico en el Ecuador ya sea por enlaces satelitales, fibra óptica o internet [16].

SEGMENTO DE ENLACE

En esta etapa se comunica la red del segmento internacional con la infraestructura clandestina a través de un enlace digital que es provisto por una empresa prestadora de servicios portadores en el Ecuador o por ciertas empresas prestadoras de servicios de valor agregado [16].

SEGMENTO DE DISTRIBUCIÓN DE LLAMADAS

Esta etapa comprende el uso de todos los elementos que permitirán el curso de la llamada desde la instalación clandestina hasta el abonado final. Aquí se envía la información a su destino mediante las líneas telefónicas adquiridas por los defraudadores; la llamada ingresa a la Central Local de Ecuador, como si se tratara de una llamada local [16].

En la Figura 1.8 podemos observar todos los segmentos que intervienen en el sistema Bypass y los actores involucrados en cada etapa.

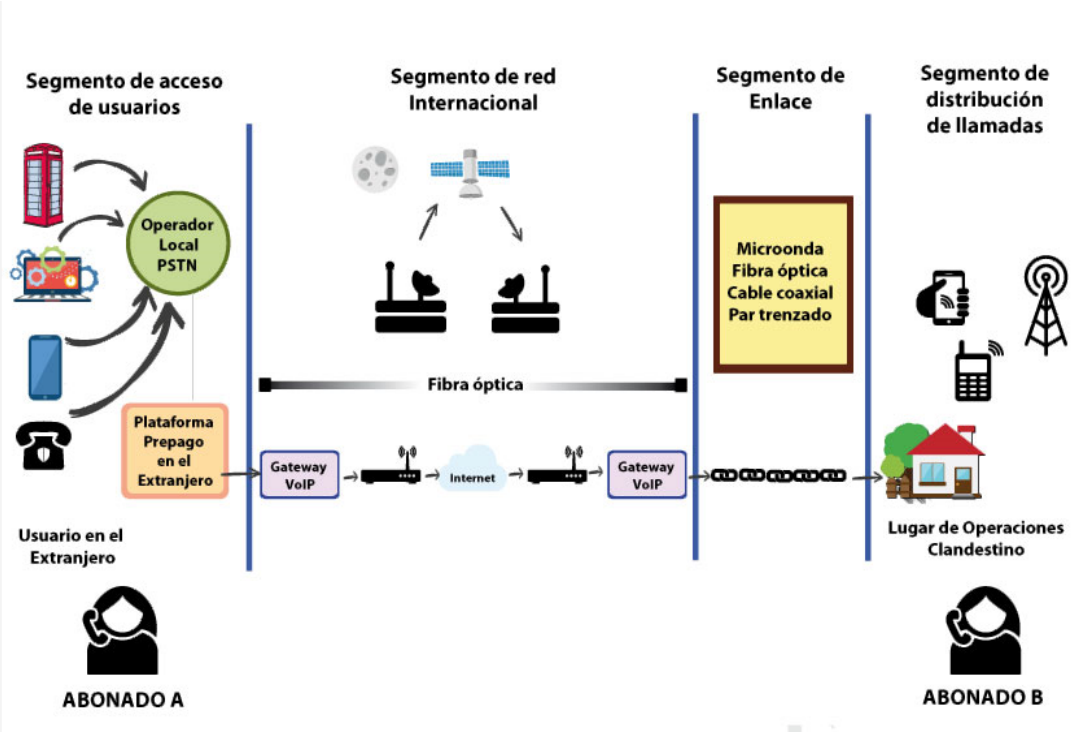


Figura 1.8: Esquema de Bypass Internacional Entrante.

BYPASS REALIZADO A TRAVÉS DE BASES CELULARES O SIMBOX

Al principio, el fraude por Bypass se cometía con teléfonos fijos, pero no fue necesario que pasara mucho tiempo para que los delincuentes se dieran cuenta de que al utilizar celulares, este delito sería más difícil de controlar debido al obstáculo que representa el encontrar la ubicación

exacta del sistema Bypass. A pesar de esto en Ecuador se ha logrado desarticular, aunque de manera poco eficiente este tipo de sistemas, prueba de esto es lo que informa el periódico “El Comercio” de la ciudad de Quito a continuación: “La Superintendencia de Telecomunicaciones (SUPERTEL), la Fiscalía de Pichincha y efectivos de la Policía Judicial intervinieron el viernes pasado una instalación de telecomunicaciones que habría sido dispuesta para cursar llamadas telefónicas internacionales no autorizadas, denominada Bypass…En ese lugar se encontraron equipos de telecomunicaciones que permitirían procesar llamadas telefónicas originadas en el exterior, las mismas eran cursadas hacia la red telefónica de la operadora Movistar. La SUPERTEL constató que para el funcionamiento de la instalación se disponía de varias líneas telefónicas utilizadas en bases celulares.” [18].

PROCEDIMIENTO PARA REALIZAR EL BYPASS A TRAVÉS DE BASES CELULARES

Tal como ocurre con el Bypass realizado con redes de telefonía fija, los estafadores que practican el enrutamiento ilegal de tráfico cursan las llamadas provenientes de otros países simulándolas como llamadas provenientes de celulares y a los precios de las tarifas impuestas por las operadoras de telefonía móvil.

“El fraude se realiza generalmente en inmuebles pequeños, en sectores con alta disponibilidad de servicios de telecomunicaciones, funcionan con poco personal (entre dos o tres personas), con dispositivos de valor mucho menor comparado con el precio de los equipos empleados por las operadoras legales. Quienes realizan Bypass negocian con los carrier para cursarles tráfico telefónico a precios más baratos que las empresas habilitadas para prestar el servicio en el País.” [16].

En una típica instalación dedicada a realizar Bypass celular podemos encontrar los siguientes elementos de red (Figura 1.9):

- Modems
- Routers
- Gateways
- Gateways GSM (Global System for Mobile)
- Teléfonos celulares cuyas líneas se encuentran a nombre de personas naturales y/o jurídicas [16].

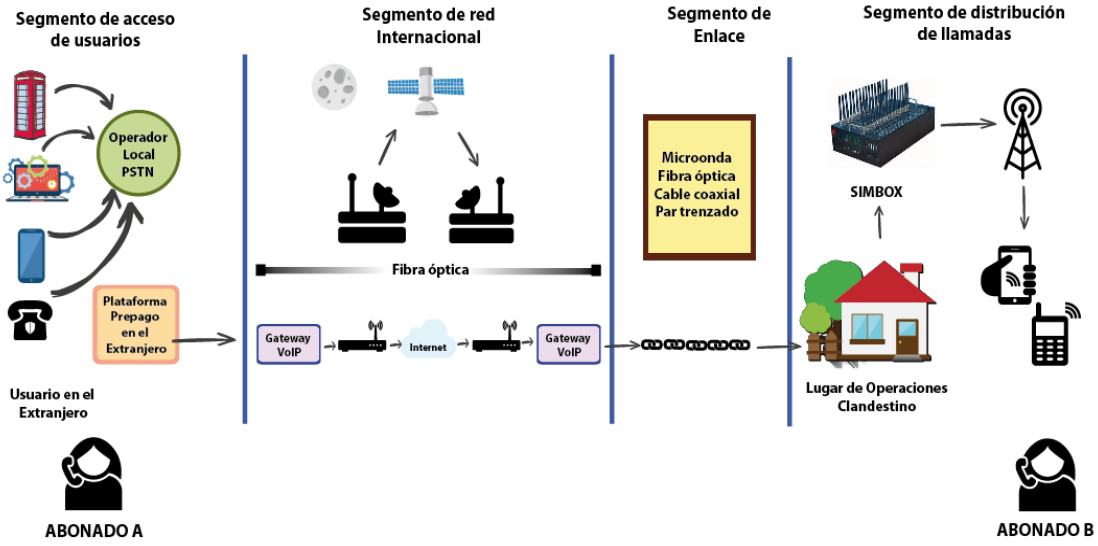


Figura 1.9: Elementos de red utilizados en las estaciones Bypass a través de bases celulares.

El fraude consiste en llamadas vía internet que son enviadas a los equipos denominados “Simbox” (máquinas que contienen tarjetas SIM, Subscriber Identity Module) encargados de redirigir el tráfico VoIP (Voice over IP) ilegal sobre las redes de telefonía móvil logrando de esta forma evitar el pago de las tarifas convencionales de interconexión pagando únicamente las tarifas de interconexión locales.

En la Figura 1.10 podemos observar una comparación entre la comunicación mediante el método legal y el método por Bypass.

Figura 1.10: Llamada entrante Internacional Bypass por líneas celulares.

BYPASS REALIZADO A TRAVÉS DE APLICACIONES PARA SMARTPHONES

Este tipo de fraude aparece como una evolución al fraude por Bypass tradicional, aunque su frecuencia de ejecución es aún menor, no pasará mucho tiempo para que se convierta en uno de los más practicados.

El Bypass a través de smartphones se lo realiza de forma similar al Bypass internacional entrante, con la diferencia de que ahora el abonado A (persona en el extranjero con smartphone e internet) realiza la llamada a un abonado móvil o fijo que no posee internet o smartphone a través de una aplicación para llamadas VoIP (generalmente Skype).

PROCEDIMIENTO:

1. El abonado A (persona en el exterior) desea llamar al abonado B (abonado fijo o móvil sin internet) desde su smartphone a través de una aplicación VoIP, generalmente Skype que le permita realizar llamadas al extranjero.

2. El abonado A, averigua las tarifas que la aplicación cobra para las llamadas a Ecuador y acredita su cuenta en la aplicación con el dinero suficiente para realizar la llamada (Figura 1.11).

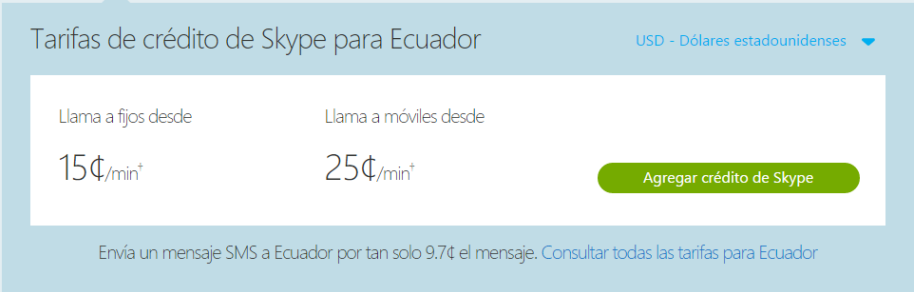


Figura 1.11: Tarifas de Skype para llamar a Ecuador [19]

Para realizar la llamada, el abonado A marca el código de área del país del abonado B, en el caso de Ecuador +593 seguido del número local.

El ISP (Internet Service Provider) del abonado A envía el tráfico de la llamada hacia el carrier encargado de enrutar la llamada.

El carrier, inducido por los bajos costos por minuto ofrecidos por el defraudador Bypass, decide enviar el tráfico por medio de la red ilícita.

La llamada entra a la red del operador legal, enmascarada como llamada nacional.

El abonado B recibe la llamada internacional, pero en su identificador visualiza un número local.

En la Figura 1.12 podemos observar cómo se ejecuta esta reciente modalidad de Bypass:

Figura 1.12: Bypass realizado a través de aplicaciones para smartphones.

BYPASS DISTRIBUIDO

Actualmente, es posible detectar un sistema Bypass a través de bases celulares mediante el grado de movilidad del chip sospechoso, es decir, cuando un chip tiene un comportamiento de llamadas atípico y permanece estático todo el tiempo (dentro de una misma celda o radio base) existe un caso de Bypass.

Con el objetivo de hacer del Bypass una práctica ilícita indetectable, surge esta variante, que realiza el mismo procedimiento del Bypass celular pero simula el movimiento en los chips del Simbox o divide geográficamente a las centrales clandestinas.

1.4.2. Clonación de celulares

Debido al incremento del robo de celulares que Ecuador vivió hace unos años, la ex SUPERTEL implementó el “Empadronamiento de teléfonos móviles”, estrategia que al principio parecía ser eficiente al combatir este tipo de delitos pero que luego logró ser burlada. “Según investigaciones

de la Policía Judicial, pese a que la Superintendencia de Telecomunicaciones (Supertel) implementó el empadronamiento de los teléfonos móviles a partir del 5 de julio del 2011 y que concluyó en la misma fecha del 2012, el robo de móviles no ha frenado.” [20].

El empadronamiento celular consiste en registrar la información del abonado (nombres, apellidos, número de cédula, dirección) y vincularla con el número de teléfono, número de IMEI (International Mobile System Equipment Identity) y tarjeta Sim de su equipo. Si el terminal móvil es robado, el dueño denuncia este delito a su operadora que bloquea el equipo y la tarjeta Sim haciéndolo inutilizable.

Pero, ¿Por qué el robo no ha sido completamente erradicado?, “Soraya Sinche, catedrática y experta en telecomunicaciones de la Escuela Politécnica Nacional, explica que sí es posible utilizar un aparato reportado como robado. Añade que al desactivar lo que se hace es bloquear el código IMEI (identidad internacional de equipo móvil), que viene de fábrica. “Luego se utilizan herramientas de software (programas informáticos) que permitan colocar otro IMEI al equipo” [20].

Estas técnicas de fraude hacen que sea posible activar en nuestro País los celulares sustraídos en el exterior o viceversa, razón por la cual la SUPERTEL ideó otra forma de contrarrestar estos delitos: “Al menos 10 millones de teléfonos celulares de los 17 millones que están activos en Ecuador tienen una procedencia supuestamente ilícita, según la Superintendencia de Telecomunicaciones, que puso en marcha un exigente sistema de registro para combatir el robo y la activación fraudulenta de esos dispositivos en colaboración con Colombia y Perú. El plan, denominado "listas positivas y negativas", arrancó el pasado 12 de marzo y se basa en un software que está en línea con instituciones colombianas y peruanas para detectar al instante los equipos robados en los países vecinos o que ingresaron de contrabando a territorio ecuatoriano.” [21].

Ahora si bien la estrategia implementada el 12 de marzo de 2014 redujo de forma significativa el contrabando de celulares entre países vecinos, ésta no ha reducido la aplicación de las técnicas de clonación de celulares para aquellos terminales robados dentro de nuestro País. Prueba de esto surge de los datos proporcionados por la ARCOTEL mediante los cuales se confirma que el robo de celulares incrementó durante los cinco primeros meses del 2015; hasta mayo las operadoras reportaron 238.423 teléfonos móviles robados, cifra que resulta superior a la registrada en el mismo período del 2014, pues en ese año ARCOTEL reportó apenas 194.527 celulares [22].

PROCEDIMIENTO PARA CLONAR CELULARES:

"La "clonación" de un IMEI se hace por medio de las cajas de liberación (o cajas unlock) de teléfonos celulares que se adquieren, en teoría, solo para activar o liberar móviles comprados en el exterior.

Existe una caja de liberación para cada marca de celular, así como las denominadas cajas semi universales como las Polar Box o la Infinity Box, que pueden funcionar con casi todos los modelos de los aparatos…...Este tipo de cajas tienen un listado completo de los IMEI de los celulares de su respectiva marca, por lo que tienen una base de datos de estos registros que les permite seleccionar cualquiera para duplicarlo e instalarlos en un celular bloqueado. El celular se conecta a la caja y este a una computadora, y por medio de un software se puede hacer el "clonado".

Dependiendo del modelo de celular, la caja tiene distintos precios...Este tipo de aparatos como los mostrados en la Figura 1.13 se pueden adquirir mediante sitios de compras por Internet, como Ebay y Amazon. También existen páginas en Internet como GSM Server o Ipart, que se dedican de forma especializada a la venta de estos sistemas.

Los expertos que trabajan en las tiendas de desbloqueo tienen una amplia experiencia para descifrar el laberinto tecnológico que hay que recorrer para sacar de la "lista negra" a un celular, pero también existen

en Internet una infinidad de tutoriales para aprender a realizar esta operación.” [23]

Figura 1.13: Cajas utilizadas para la liberación de las diferentes marcas de celulares.

1.4.3. Fraude de Tercer País

Este tipo de fraude utiliza varias líneas telefónicas para realizar la comunicación entre dos usuarios de diferentes países, además de la intervención de un tercer país con una menor tarifa [14].

El fraude de Tercer País consiste en que el usuario que origina el tráfico procede a enrutarlo a un país intermediario, que se encarga de recibirlo y por medio de una llamada en conferencia o un conmutador, redirige el tráfico al usuario final en otro país (Figura 1.14) [24].

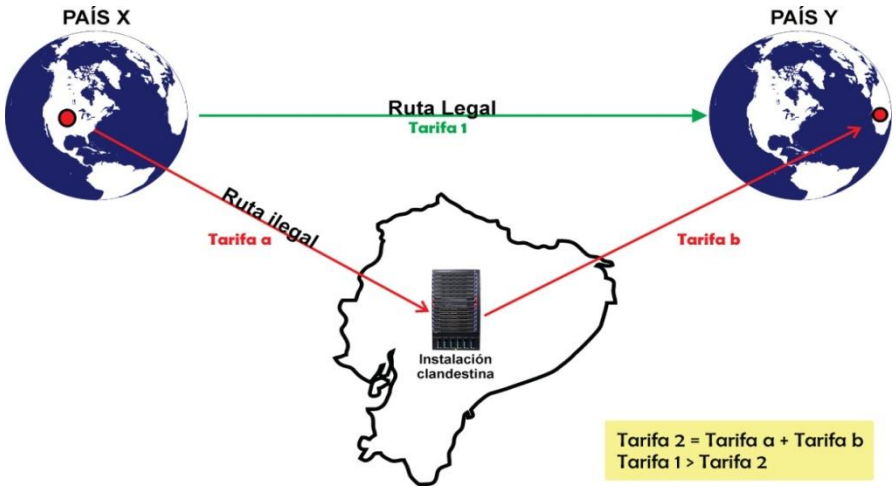


Figura 1.14: Diagrama del Fraude de Tercer País

Este fraude afecta, por lo general, a dos de los tres países involucrados. El defraudador en el país intermediario debe conseguir una o varias líneas telefónicas locales para establecer la comunicación, esto lo puede realizar presentando documentos falsos a la compañía o por medio de algún método de evasión, para que las llamadas facturadas no sean cobradas por la operadora. Debido a la diferencia en las tarifas entre el país origen y país destino de toda la comunicación, el último recibe el pago de una tasa más baja que se proyecta como menores ingresos a dicho país [24] [25].

Otra forma de realizar este fraude es cuando el país intermediario genera tráfico saliente para ambos países y luego los interconecta, este método resulta sumamente perjudicial para la compañía en dicho país porque el estafador elude el pago del tráfico registrado [24] [25].

1.4.4. Hackeo de centrales PBX

Una PBX (Private Branch Xchange) es una red de telefonía privada usada dentro de una empresa que conmuta las llamadas locales entre los usuarios en la empresa mientras que permite el uso de extensiones telefónicas para facilitar la comunicación. La central de la PBX es de propiedad de esta empresa y no de una compañía telefónica [26].

El hackeo de centrales PBX tiene diferentes modos de originarse que a continuación presentamos con detalle

*La Ingeniería social.***-** Los hackers se conectan a un número dentro de la empresa y emplean excusas para ser transferidos de nuevo al operador. De esta manera el operador ve la llamada como una llamada interna y es persuadido para ayudar a que el hacker realice una llamada a un número externo o internacional [26].

Contestador automático.- Los hackers pueden ser capaces de obtener acceso no autorizado al sistema telefónico a través del sistema de correo de voz. Esto les permite realizar llamadas no autorizadas de alto

costo, volver a grabar mensajes de bienvenida y bloquear a los usuarios legítimos [26].

Acceso a través de los puertos de mantenimiento del sistema.- Los puertos de mantenimiento en una plataforma PBX o correo de voz permiten a los ingenieros configurar el equipo. Si un hacker PBX tiene acceso a este puerto, puede ser capaz de reconfigurar el sistema y permitir aquellas llamadas de larga distancia no autorizadas [26].

Desvíos de llamada, llamadas en conferencia, Espiar conversaciones.- Si un hacker PBX puede acceder al puerto de mantenimiento o administrativo en un sistema PBX, también es posible [26]:

- Espiar todas las conversaciones que tienen lugar en toda la red.
- Desviar de llamadas a otro lugar (por ejemplo, casa, móvil o en el extranjero), cuando el propietario de la extensión está ausente.
- Configurar llamadas en conferencia remotamente.

Acceso a través del servicio de acceso DirectInward.- Esta es una característica que permite a los empleados que trabajan fuera de la oficina para hacer llamadas a través del sistema telefónico de su empresa. Los hackers PBX pueden utilizar esta función para hacer llamadas de alto costo no autorizado a un número de terminación de su elección si éste no está configurado correctamente [26].

En las Figuras 1.15 y 1.16 podemos observar las diferencias entre una central PBX sin alterar y una PBX que ha sido vulnerada a través del método de transferencia de llamada.

Figura 1.15: Esquema de una PBX sin alterar.

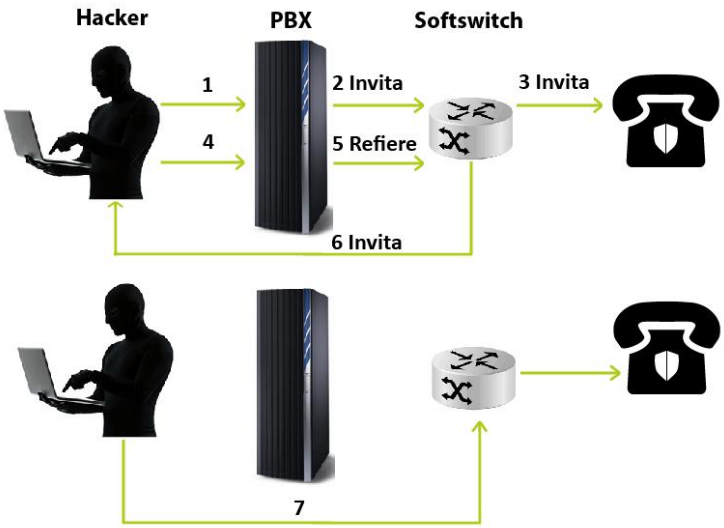


Figura 1.16: Esquema de una PBX hackeada por el método de transferencia de llamada.

1.4.5. Refilling

El Refilling o “Re-enrutamiento” es una evolución del fraude de tercer país, que básicamente operan de igual forma, es decir, el tráfico de un país X es dirigido al país Z para luego ser enrutado ilegalmente hacia el país Y, todo esto con el propósito de obtener una tarifa más baja que genera menores ingresos al país destino Y.

Este fraude se lo puede realizar utilizando el hackeo de las centrales PBX-IP, donde el defraudador tiene acceso a la central mediante el puerto IP de la misma y a través de ella puede realizar llamadas como se lo muestra en la Figura 1.17. Los sistemas refilling con Voz sobre IP, están estructurados de igual forma que el Bypass y el fraude por hackeo PBX-IP, descritos anteriormente, con la diferencia de que estos no terminan las llamadas internacionales dentro del país, sino que hacen uso de los recursos de la operadora en el país intermedio para finalizar la llamada en el exterior [27].

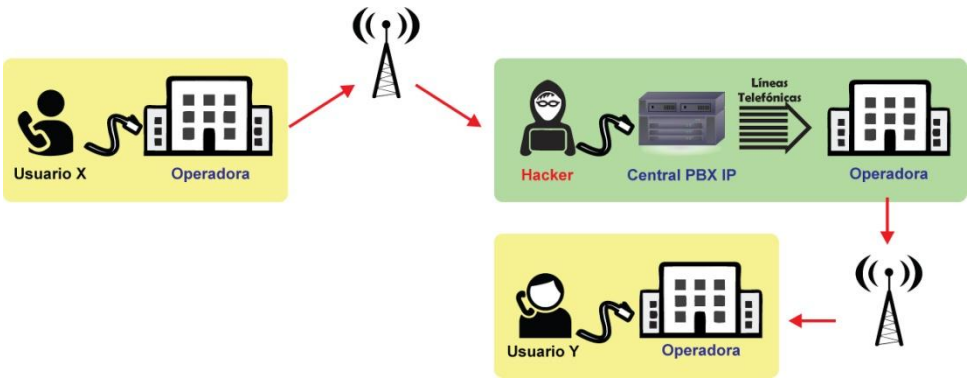


Figura 1.17: Diagrama de Refilling por Voz sobre IP

Según el Ingeniero Darwin Pérez de la ARCOTEL, el Refilling puede llegar a generar grandes pérdidas, incluso mayores que las producidas por Bypass, por las llamadas realizadas a destinos considerados peligrosos y con una tarifa de minutos muy alta.

1.4.6. Fraude por roaming

Como una de las nuevas tendencias, surge el fraude por roaming, en el que un defraudador adquiere chips del extranjero con el servicio de roaming habilitado utilizando documentos falsos y los emplea dentro de un determinado país con el fin de realizar llamadas en la red de la operadora local sin la intención de pagarlas [14].

PROCEDIMIENTO

- El dueño de un sistema Bypass adquiere en el extranjero los chips que utilizará dentro de su central telefónica celular clandestina.
- Establece un contrato de roaming con la operadora de ese país utilizando documentos falsos.
- Regresa a su país de origen y utiliza los chips en su sistema Bypass, generando tráfico en las operadoras locales.
- La operadora local identifica al número que genera el tráfico como “visitante” y enmascara el chip con un número comodín propio del servicio de roaming. En esta etapa se pueden identificar dos casos:

  La llamada termina en la red del mismo operador local

  Para este caso la operadora local le cobra a la operadora extranjera el servicio de interconexión por roaming.

  Cuando la operadora extranjera intenta cobrar los gastos producidos al dueño de los chips, descubre que los documentos utilizados por el suscriptor son falsos, ocasionando pérdidas significativas.

  La llamada termina en la red de un operador local diferente

  Cuando se percibe un caso así es cuando surgen los problemas, pues el operador local donde termina la llamada detecta el fraude Bypass y al observar el número comodín, descubre que el delito

está siendo provocado por otra operadora local, generando discrepancias legales entre ambas entidades.

Este fraude está catalogado como peligroso, pues perjudica no solo a la operadora local que debe enfrentar malos entendidos al proceder con la interconexión cuando la llamada termina en la red de una operadora diferente, sino también a la operadora extranjera que debe asumir todos los cargos causados por el falso suscriptor. Para tener una idea clara de cómo se ejecuta este fraude, en la Figura 1.18 podemos observar el diagrama de fraude por Roaming con todos sus elementos involucrados [14].

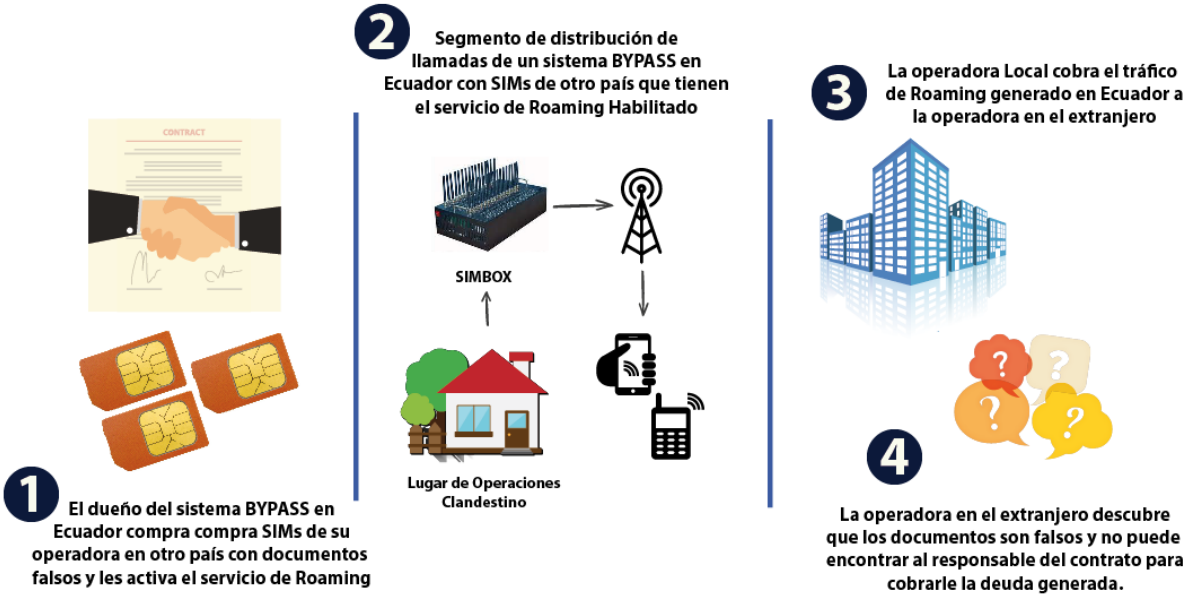


Figura 1.18: Diagrama de Fraude por Roaming

1.4.7. Falsa Respuesta a llamada

Conocida como FAS, este tipo de fraude simula un servicio de llamadas a números que están fuera de su red de cobertura y ofrece falso tiempo aire para hablar mediante tarjetas prepago físicas o en línea, usualmente, al extranjero [28].

Cuando no se puede establecer una conexión entre los usuarios, la persona que realiza la llamada debe ser notificada, mediante una breve grabación, que no hay respuesta de la línea con la que intenta comunicarse y como la llamada no se completa, no debe facturarse o generar algún tipo de cargo a la cuenta o tarjeta adquirida por el usuario; sin embargo, los estafadores utilizan esa respuesta para hacer que las llamadas aparezcan como completadas y proceder a realizar el cobro de las mismas [29].

En la Figura 1.19 se muestra un escenario típico de este fraude, el proceso inicia cuando el suscriptor realiza la llamada, que es procesada por el IVR (Interactive voice response) para que pueda ingresar el código que lo identifica como usuario de la compañía defraudadora, luego la operadora asigna el tráfico a su respectivo carrier o proveedor de enrutamiento; dentro de la gran red de carriers el defraudador, sin conexión a la operadora que tiene la línea destino en su red, toma la llamada proveyendo de una respuesta falsa, esto es una grabación que mantendrá al usuario en espera, propagandas, ruido exterior, entre otras; esto hará que la llamada finalice en su red y poder cobrar la tarifa respectiva.

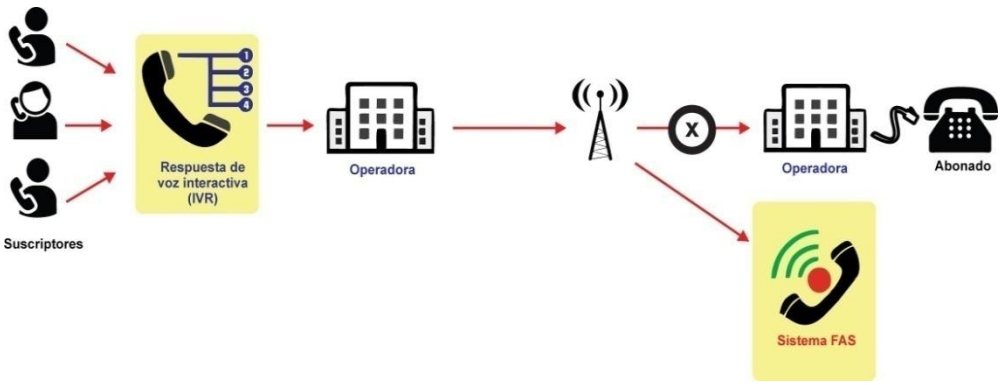


Figura 1.19: Escenario de Falsa Respuesta a llamada

Cuando una red Bypass es descubierta y las líneas son bloqueadas, el cómplice en el extranjero del fraude mencionado, suele incurrir en el delito por FAS para así intentar evitar las pérdidas ocasionadas por la detección del primer intento de fraude.

1.4.8. Fraude por OTT

Aquello servicios multimedia de voz, audio, video, etc, que son ofrecidos por entidades ajenas a las operadoras tradicionales de telecomunicaciones, se los consideran servicios OTT, ejemplo de ellos son Whatsapp, Facebook messenger, Skype, Viber y entre otros [30].

Este nuevo desarrollo de la tecnología es una preocupación para los operadores de telefonía, puesto que las aplicaciones han comenzado a competir directamente con los servicios ofertados por las operadoras como son los de voz y mensajería [30].

Algunos desarrolladores de las aplicaciones OTT han ingresado al mercado actuando como portadores internacionales, de modo que también pueden ofrecer servicios de terminación de llamadas en sus aplicaciones, en lugar de los servicios básicos de telefonía [31].

Un ejemplo de esto se da con la aplicación Viber (Figura 1.20) que ofrece los servicios OTT de voz, mensajes y video de extremo a extremo, es decir que ambos usuarios estén dentro de la aplicación y servicio de voz saliente para usuarios finales fuera de su red; la aplicación cuenta con más de 200 millones de usuarios [32].

La aplicación ya ha empezado a probar el modelo económico; en el 2013 los representantes de la aplicación confirmaron al portal web TechCrunch, que se estaban ejecutando pruebas que permitirían realizar la terminación de llamadas, de este modo sus accionistas logran obtener mayor beneficio económico [33]; pero cualquier aplicación con un gran número de suscriptores puede acceder a este mercado.

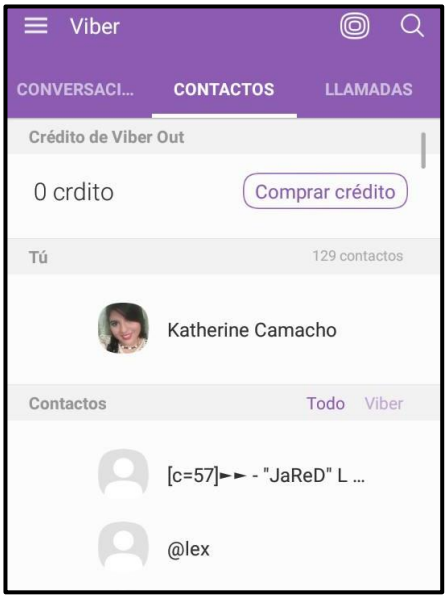


Figura 1.20: Aplicación Viber Móvil

En el proceso tradicional de comunicación telefónica, una llamada origina el pago de una tarifa determinada que se traduce en ganancia para la operadora y demás agentes de telecomunicaciones que intervienen en la conexión; el uso de las aplicaciones OTT pone en riesgo sus ingresos, pero esto no lo convierte en fraude [34].

El fraude por OTT se da cuando los defraudadores interceptan llamadas telefónicas normales y deciden terminarlas a través de un entorno IP mediante la aplicación asociada con el acto ilícito, instalada en el dispositivo y activa en el momento que se realiza la llamada; de esta forma la operadora local no puede cobrar el costo por interconexión.

El procedimiento de este fraude se lo muestra en la Figura 1.21, el abonado realiza la llamada que sale desde la operadora hasta su carrier de servicio, muchas veces este u otro carrier de la gran red hace contacto con el administrador de cierta aplicación para poder enviar el tráfico a través de la red IP y así no facturar cargos adicionales. La OTT debe verificar en su base de datos si contiene el número destino, que lo obtienen cuando el usuario se registra en dicha aplicación, y si se

encuentra activo (con red de datos) en el momento que se desea establecer la conexión, con estos datos esenciales, el defraudador envía el paquete de datos como VoIP y por medio de la aplicación al usuario destino, causando un perjuicio económico al país donde la comunicación debería terminar, puesto que la llamada origen usa un recurso del Estado (593) que es aprovechado por terceros para su propio beneficio.

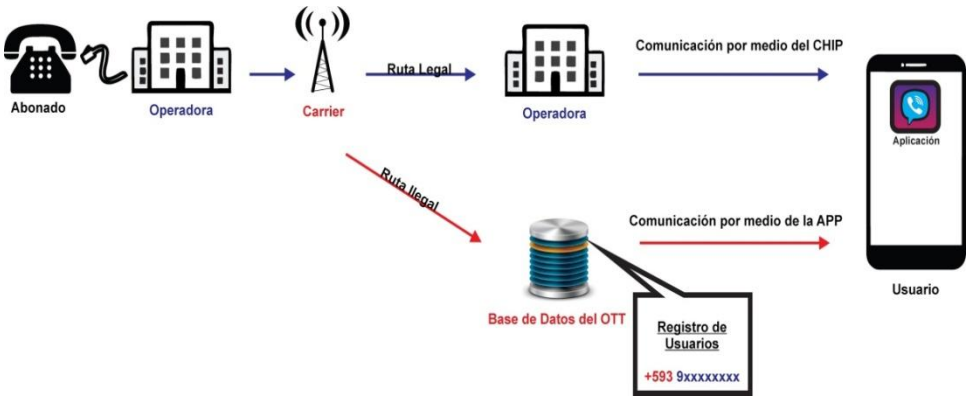


Figura 1.21: Diagrama de fraude por OTT.

Por ejemplo, en la Tabla 2, se muestra la comparación entre las tarifas aproximadas que pueden ser cobradas al usuario final, de modo que es visible la pérdida que resulta de una llamada terminada vía IP, es decir por medio de la aplicación. Los costos de facturación son calculados en base a un consumo de 497 KB/min por la aplicación Viber [31] y las tarifas cobradas por CONECEL.

TARIFA APLICADA	PRECIO DE FACTURACIÓN
Datos: **$0.224 por MB**	$0,108
Terminación de llamadas: **$0,00**	$0,00

Tabla 2: Cobro por recepción de llamadas con la red de datos móvil

1.4.9. Fraude de Suscripción

Hoy en día, esta forma de fraude busca suplantar la identidad de terceras personas con el propósito de adjudicarles el pago de los servicios de telecomunicaciones, de los cuales otros se beneficiaron. De esta manera, el fraude de suscripción afecta tanto al usuario, que puede llegar a ser registrado moroso y perjudicar su historial crediticio, como a la operadora que no cobra por el consumo que se realizó en la línea telefónica [24] [35].

La Figura 1.22 muestra el proceso de este tipo de delito, donde el defraudador proporciona información falsa a la operadora, que procederá a brindar el servicio.

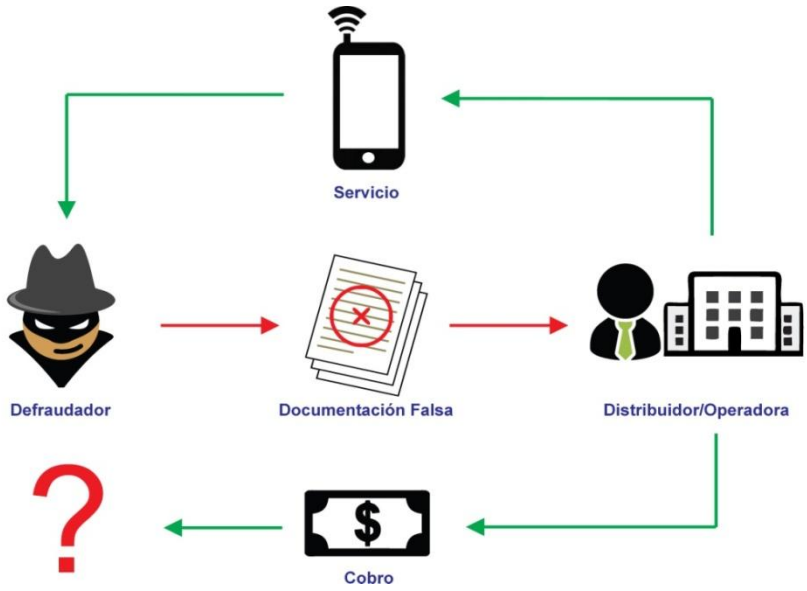


Figura 1.22: Diagrama del Fraude de Suscripción.

En el área de los servicios móviles avanzados es más común este tipo de delito; el libro “FRAUDE EN LAS TELECOMUNICACIONES” menciona que “La telefonía móvil estimula el fraude de suscripción (a través de documentos falsos), al facilitar el mentir al respecto de la información personal” [35].

1.4.10. Fraude Interno

Debido al conocimiento de los sistemas, procesos y la facilidad de acceso a la información que tienen los empleados de las empresas que prestan servicios de telecomunicaciones, el fraude interno es uno de los delitos más intangibles [36].

Este tipo de fraude puede darse desde cualquier parte del proceso organizacional de la empresa como en la administración de servicios de facturación, base de datos de los clientes donde se puede crear cuentas falsas o alterar su información, plataformas de administración de pagos, entre otros [36].

A continuación se explica con detalle los métodos de fraude interno más comunes en el país.

GHOSTING

El fraude de ghosting se produce cuando se llega a manipular la red con el propósito de alterar la producción, acreditación de saldo por medio de recargas no autorizadas, distribución ilícita de los códigos secretos de las tarjetas prepago, modificación de los registros de llamadas (Call Detail Records) de los clientes (información de la base de datos como nombres, direcciones, consumo de llamadas, categoría de abonados, etc) [5].

Esta forma de fraude resulta perjudicial porque al realizar alteraciones se puede evitar el cobro de las facturas o poner a disposición de terceros la información confidencial de la empresa [36].

MANIPULACIÓN DE ARMARIOS Y ROBO DE LÍNEAS TELEFÓNICAS

La persona que efectúa este tipo de fraude, accede a los armarios telefónicos de las operadoras para manipular el sistema, realizando conexiones no autorizadas de líneas telefónicas, cuyas llamadas serán facturadas al dueño de la línea que ha sido usada ilegalmente [5].

1.5. Impacto del Fraude en telefonía fija y móvil

Debido al desarrollo de los servicios de telefonía, tanto fija como móvil en el Ecuador, se han reducido las tarifas y costos de los mismos, pero esto no ha logrado erradicar el cometimiento de fraudes en dicho ámbito.

Según la CFCA, se estima que lo ingresos globales en servicios de telecomunicaciones son de $2.25 trillones anuales, las pérdidas por fraudes representan el 1,69% de este valor, es decir $38.1 billones, distribuidos de acuerdo al tipo de fraude según la Figura 1.3 de la sección 1.

El efecto negativo que ocasiona el fraude en la telefonía tiene repercusiones tanto en las operadoras, como en los usuarios y el Estado [37].

El usuario es afectado cuando es víctima de algún tipo de suplantación de identidad, cuyo cometido es hacer que este pague por el tráfico ilegal cursado a través de su línea. El perjuicio ocasionado no es sólo a nivel económico, sino que también se refleja en la imagen del estafado, que puede llegar a caer en central de riesgo crediticio por la deuda que se le ha atribuido de forma ilícita [37].

El Impacto jurídico debido al fraude, afecta negativamente al usuario y a la operadora, pero repercute en mayor grado al primero pues debe demostrar ante la justicia su inocencia si se ve inculpado en actos dolosos [37].

Con las pérdidas que ocasiona el fraude en la telefonía, las rentas del Estado proveniente del pago de impuestos y contribuciones especiales que generan los servicios de telecomunicaciones disminuyen. Esto repercute en la inversión, por ejemplo la que se realiza por medio del FODETEL u otros organismos estatales, para proveer de servicios de telecomunicaciones a las zonas rurales y urbano-marginales [37].

Además de la reducción de ingresos que ocasionan ciertos tipos de fraudes, las estafas que afectan directamente al usuario pueden llegar a perjudicar la imagen pública de la operadora de telecomunicaciones, al ser vinculado como

copartícipes de este tipo de actos ilícitos, para generar mayores ingresos a cuestas del agravio a sus abonados [37].

Según reuniones mantenidas con un ex-funcionario del Departamento de Aseguramiento de Ingresos en Claro, esta empresa reportó un golpe duro a su economía al registrar una pérdida de cerca de 3 millones de dólares entre el 2008 y 2010 debido al fraude interno con tarjetas prepago, pues ciertos empleados que tenían acceso a las bases de datos de los códigos impresos en las tarjetas, aprovecharon la debilidad del sistema y lograron lucrarse a partir de la venta de los mismos de manera particular.

Algo parecido al fraude interno de tarjetas prepago resultó ser el fraude por recargas electrónicas fraudulentas, en el cual, algunos asesores autorizados para recargar valores de prueba (típicamente de un costo muy pequeño) en plataformas de trabajo, abusaron de su rol dentro de la empresa y empezaron a realizar recargas de cantidades altas a números ajenos a la plataforma de prueba, produciendo así cuantiosas pérdidas económicas para esta operadora.

Los distribuidores constituyen las principales fuentes de ingreso de las operadoras públicas y privadas al encargarse de suscribir a nuevos abonados diariamente, el conflicto económico se manifiesta cuando los datos suministrados al momento de registrar a los clientes de una red son ficticios; según la versión proporcionada por el funcionario entrevistado, existen contramedidas efectivas que logran detectar el fraude por identidad falsa (detalladas en el capítulo 2), sin embargo, éste sigue siendo uno de los delitos más cometidos en la actualidad.

Para Claro, el Bypass representó una de las mayores amenazas para las operadoras de telefonía fija y móvil entre los años 2000 - 2008, provocando el mayor porcentaje de pérdidas económicas registradas durante ese período. La falta de automatización de los sistemas de detección y la falta de información provocó que este delito se convirtiera en la mayor causa de los perjuicios económicos reportados por año. Seguidos de él se encontraban el fraude interno y por suscripción.

Posteriormente, en los años 2010-2014 los sistemas de detección del Bypass se automatizaron, por lo que su práctica disminuyó considerablemente, además la aparición de nuevas aplicaciones de VoIP para llamadas internacionales gratuitas (Whatsapp, viber, etc) redujo la necesidad de comprar las tarjetas pre pagadas y por ende el Bypass. El escenario no fue el mismo para el fraude por suscripción que aumentó ligeramente en este período debido a la facilidad que representó para los infractores cometer este delito.

La clonación de IMEIs empezó a ganar importancia en el 2010, los robos y contrabando de celulares entre las fronteras tomaron impacto generando pérdidas a las operadoras de telefonía móvil, mientras que el fraude interno a lo largo de todos estos años no ha dejado de ser practicado, conforme el personal deshonesto es separado de la operadora, siempre existen nuevos empleados que se dejan corromper por la idea de generar dinero extra a partir de la información confidencial que la empresa en la que trabajan pone en sus manos.

1.6. Objetivos

1.6.1. Objetivo General

Este proyecto de carácter investigativo y técnico derivará en el diseño de dos sistemas basados en las actuales plataformas antifraude implementadas por las operadoras de telefonía en el Ecuador, para fortalecer la detección y control de las nuevas tendencias de fraude por Bypass y OTT, mejorando así los procesos de control de las actividades ilícitas en los sistemas de telefonía fija y móvil en el país.

1.6.2. Objetivos específicos

- Identificar los nuevos métodos y tecnologías utilizadas para efectuar fraude en los sistemas de telefonía fija y servicios móviles avanzados.
- Analizar las estrategias empleadas por las prestadoras de servicios de telecomunicaciones y la Agencia de Control y Regulación de las Telecomunicaciones en el Ecuador para minimizar las pérdidas ocasionadas por los diversos tipos de fraude.
- Diseñar sistemas empleando herramientas accesibles que complementen las estructuras de detección y control del fraude en la telefonía fija y móvil, para permitir la identificación de nuevas técnicas ilícitas que se están desarrollando tanto dentro como fuera del país.

1.7. Justificación

Todas las empresas de telecomunicaciones están expuestas a diversas formas de fraude que les causan cuantiosas pérdidas económicas y los efectos de estos actos ilícitos llegan a perjudicar también a los usuarios y al Estado ecuatoriano.

La evolución de la tecnología, el fácil acceso a equipos de telecomunicaciones, la creación de nuevas aplicaciones y metodologías de comunicación, han motivado el desarrollo de las técnicas de fraude, de modo que las estrategias comunes de detección no bastan para identificar los actos fraudulentos cometidos.

En el Ecuador se están desarrollando estas nuevas modalidades, pero no se han tomado las medidas necesarias para controlarlas, esto provocará el aumento de las posibilidades y frecuencia con que se cometen estos delitos, que podría generar un gran perjuicio tanto a operadoras, usuarios y al Estado, en el futuro inmediato.

1.8. Alcance del proyecto integrador

Las operadoras y ARCOTEL invierten en equipos y sistemas especializados para combatir las ilegalidades en Telecomunicaciones; sin embargo, la evolución tecnológica provoca la aparición de nuevas estrategias de fraude, que logran burlar los métodos de detección, provocando el aumento de las posibilidades y frecuencia con que se cometen estos delitos.

La automatización de los sistemas de detección implementados por las operadoras, la aparición de empresas internacionales encargadas de detectar el fraude y el auge de las aplicaciones gratuitas para la comunicación a distancia redujeron drásticamente la práctica del Bypass, pero no la erradicaron, lo que en realidad lograron es que el Bypass evolucione de tal forma que actualmente se lo realiza en las aplicaciones de telefonía móvil más usadas como: Whatsapp, Viber, Line, entre otras. Esta nueva variación podría convertirse en la nueva preocupación de las operadoras, por lo que resulta fundamental encontrar un método idóneo y automatizado que logre controlar esta actividad.

Una vez analizados todos los métodos de detección utilizados en Ecuador, podemos constatar que el avance en la tecnología y la evolución de las actividades ilícitas provocan la necesidad de establecer estrategias más innovadoras y eficientes, por lo que con este proyecto integrador se pretende analizar el procedimiento de los sistemas de detección y control del fraude en los servicios de telefonía fija y los servicios móviles avanzados para aportar con sugerencias de diseño enfocados a complementar los sistemas ya implementados por las operadoras para detectar el Bypass desde smartphone, que afecta en su mayoría a los proveedores de telefonía fija y el fraude por OTT que perjudica a los proveedores de telefonía móvil.

CAPÍTULO 2

2. SISTEMAS DE DETECCIÓN Y CONTROL DEL FRAUDE EN SERVICIOS DE TELEFONÍA FIJA Y MÓVIL

Con el afán de frenar las pérdidas ocasionadas por los fraudes en los servicios de telefonía fija y móvil previamente mencionados, las operadoras privadas y públicas así como la ARCOTEL cuentan con los Departamentos de Aseguramiento de Ingresos encargados de emplear diversas técnicas antifraude que ayuden a detectar de forma eficiente los delitos cometidos día a día.

Para ello hacen uso de una práctica basada en el ciclo de vida de la gestión del fraude, mostrado en la Figura 2.1, que se encuentra dividido en etapas que exponen su dinamismo y adaptación.

Figura 2.1: Ciclo de vida de la Gestión del Fraude.

La ARCOTEL y las operadoras telefónicas comparten cierta información técnica y administrativa de las líneas telefónicas que presenten actividad irregular, de modo que se pueda detectar la localización exacta de la instalación clandestina y conseguir las pruebas pertinentes para el debido proceso legal; todo esto es

gracias al “Convenio único de cooperación y apoyo para facilitar el combate de ilícitos en telecomunicaciones”, firmado en el 2011 por la ex SUPERTEL y operadoras, el cual sigue vigente hasta la presente fecha [38].

2.1. Criterios de Detección y Estrategias de Prevención por tipo de fraude

Un apropiado análisis de la información, que se obtiene de los CDRs (Call Detail Records), datos administrativos y demás recursos estadísticos de la operadora, permite diferenciar los casos probablemente fraudulentos y así minimizar el tiempo y recursos en falsas alarmas, enfocándose en la detección de los ilícitos.

Como contramedida a los perjuicios económicos que los diferentes tipos de fraude ocasionaron, las operadoras han desarrollado criterios de detección y estrategias de prevención según los más comunes en el Ecuador, analizados previamente en el capítulo 1.

2.1.1. Bypass

El Bypass fue uno de los procedimientos fraudulentos más practicados desde su aparición. Para las operadoras basta que un sistema Bypass opere tan solo dos días en sus redes para que se produzcan pérdidas millonarias hasta lograr detectar esta anomalía en sus registros.

Para detectar el Bypass y todas sus últimas evoluciones, los funcionarios de los departamentos de aseguramiento de ingresos de las diferentes operadoras de telefonía fija y móvil, basan sus análisis en los siguientes parámetros obtenidos a partir de la lectura exhaustiva de los CDRs (explicados con detalle más adelante) de los cuáles se establecen los siguientes indicadores de fraude:

- Descensos abruptos en las llamadas internacionales entrantes.
- Aumento de las llamadas locales.
- Llamadas prolongadas realizadas en horarios inusuales (horas de la madrugada).
- Grado de movilidad del chip muy bajo (chips estáticos).

- Usuarios que registran más de 10 líneas telefónicas.
- Chips que no reciben llamadas.

Gracias a ellos, se puede filtrar la información para obtener todos los chips implicados en casos de Bypass, y tomar las medidas correctivas necesarias [14].

2.1.2. Clonación de celulares

La forma más básica de detección es cuando el usuario realiza el reporte de robo o pérdida de su teléfono celular, luego el IMEI clonado es identificado cuando se realiza alguna actividad y se procede a bloquear las llamadas desde y hacia el mismo. Otro indicador de este tipo de fraude se da cuando el usuario percibe que los valores en su factura aumentan y se le realizan cobros de llamadas que no realizó [14].

Este fraude puede ser detectado por la compañía celular al realizar un seguimiento de actividades entre chips y equipos basados en parámetros propios de cada operadora; el cierre de una línea que ha sido clonada en numerosas ocasiones representa una afectación económica a la operadora, por lo cual se están estudiando procedimientos que permitan diferenciar el usuario original de los clones para evitar los perjuicios que se puedan originar [14].

Como norma de prevención, la ex SUPERTEL implementó el empadronamiento de celulares y recomienda a los usuarios reportar la pérdida de sus equipos a los proveedores de servicio para realizar el respectivo bloqueo [14].

2.1.3. Fraude de tercer país

Es común que al detectar números que están siendo usados en sistemas Bypass también sean usados para este tipo de fraude; sin embargo, para realizar un control más riguroso y específico, los

organismos utilizan técnicas que permiten cuantificar estadísticamente el tráfico telefónico internacional cursado hacia los demás países, de tal forma que al notar un aumento significativo no justificado de dicho tráfico hacia un destino en particular, se pueda detectar el fraude de tercer país [14].

Es posible determinar el número que origina las llamadas fraudulentas y con información de los mismos, localizar la infraestructura de telecomunicaciones usada para el fraude [14].

2.1.4. Hackeo PBX en Ecuador

Algunos indicadores que demuestran la presencia la de un hacker dentro de una central PBX o PBX IP podrían ser los enlistados a continuación [39]:

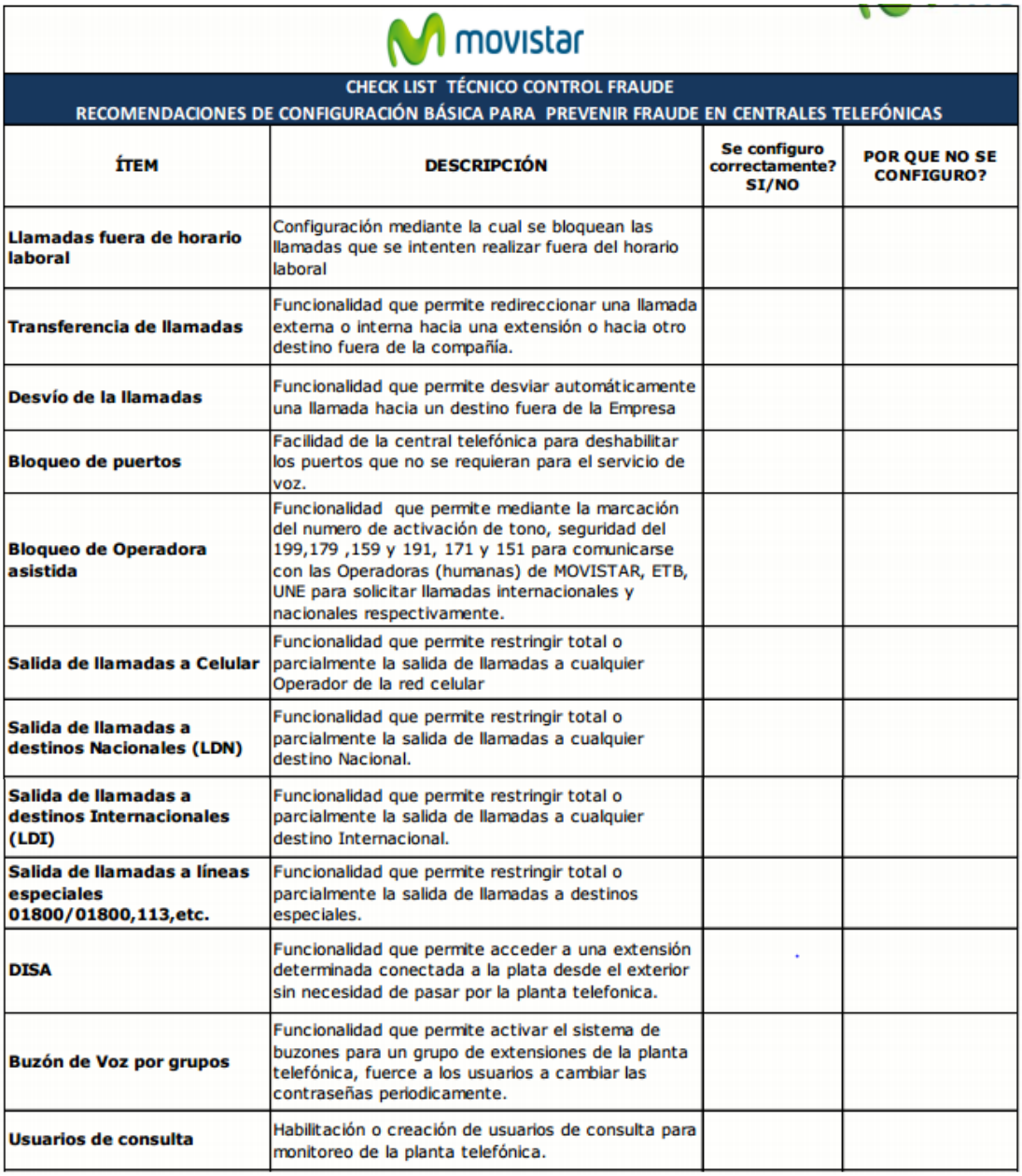
- Facturas de servicio telefónico demasiado elevadas.
- Mala calidad de las llamadas (posible espionaje).
- Tráfico atípico de llamadas internacionales salientes.
- Realización de llamadas durante los días en que la empresa no labora.
- Incremento de llamadas desde extensiones poco usadas.
- Funcionalidades que antes estaban deshabilitadas dentro de la red, ahora son de libre acceso para todos los usuarios.

Debido a que la detección de este tipo de fraude no ocurre sino hasta cuando se producen pérdidas económicas notables, las diferentes empresas públicas y privadas centran sus esfuerzos en mantener la central segura a través de los siguientes procedimientos de rutina [39]:

- Asegurarse de que las características de seguridad disponibles están encendidas.

- Administrar responsablemente todos los puertos de administración estableciendo todos los protocolos de seguridad posibles.
- Insistir en que los equipos sigan los procedimientos de seguridad básicos.
- Usar un monitor de llamada a nivel de aplicación, es decir, aquellos que chequean los paquetes generados durante una llamada en tiempo real, con el objetivo de buscar el tráfico inusual que pudiera indicar actividad fraudulenta en la red, tanto desde dentro (personas con acceso nocturno al establecimiento de costosas llamadas de tarifa internacional y Premium) y externo (la intención de hackers en el uso de la red para que actúe como central de su sistema Bypass generando así llamadas internacionales a muy bajo costo) [39].
- Hacer buen uso de servidores de seguridad y controladores de sesiones fronterizas.
- Usar registro de llamadas en línea y análisis de facturación para buscar propensión al fraude.

En Colombia la operadora Movistar previene el hackeo PBX en las redes de sus clientes mediante checklists técnicos (Figura 2.2) como el enlistado a continuación [40]:



movistar

CHECK LIST TÉCNICO CONTROL FRAUDE RECOMENDACIONES DE CONFIGURACIÓN BÁSICA PARA PREVENIR FRAUDE EN CENTRALES TELEFÓNICAS			
ÍTEM	**DESCRIPCIÓN**	**Se configuro correctamente? SI/NO**	**POR QUE NO SE CONFIGURO?**
Llamadas fuera de horario laboral	Configuración mediante la cual se bloquean las llamadas que se intenten realizar fuera del horario laboral		
Transferencia de llamadas	Funcionalidad que permite redireccionar una llamada externa o interna hacia una extensión o hacia otro destino fuera de la compañía.		
Desvío de la llamadas	Funcionalidad que permite desviar automáticamente una llamada hacia un destino fuera de la Empresa		
Bloqueo de puertos	Facilidad de la central telefónica para deshabilitar los puertos que no se requieran para el servicio de voz.		
Bloqueo de Operadora asistida	Funcionalidad que permite mediante la marcación del numero de activación de tono, seguridad del 199,179 ,159 y 191, 171 y 151 para comunicarse con las Operadoras (humanas) de MOVISTAR, ETB, UNE para solicitar llamadas internacionales y nacionales respectivamente.		
Salida de llamadas a Celular	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier Operador de la red celular		
Salida de llamadas a destinos Nacionales (LDN)	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier destino Nacional.		
Salida de llamadas a destinos Internacionales (LDI)	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier destino Internacional.		
Salida de llamadas a líneas especiales 01800/01800,113,etc.	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a destinos especiales.		
DISA	Funcionalidad que permite acceder a una extensión determinada conectada a la plata desde el exterior sin necesidad de pasar por la planta telefonica.		
Buzón de Voz por grupos	Funcionalidad que permite activar el sistema de buzones para un grupo de extensiones de la planta telefónica, fuerce a los usuarios a cambiar las contraseñas periodicamente.		
Usuarios de consulta	Habilitación o creación de usuarios de consulta para monitoreo de la planta telefónica.		

Figura 2.2: Checklist técnico establecido por movistar Colombia para prevenir fraude en centrales PBX. [40]

2.1.5. Refilling

Los indicadores para detectar el fraude de re-enrutamiento que se pueden encontrar en los registros de tráfico telefónico internacional saliente son [14]:

- Registros de llamadas dirigidas a destinos pocos comunes, por ejemplo: Somalia, Cuba, países de medio oriente, entre otros.
- Aumento en el consumo de llamadas internacionales.

Una vez verificado los datos administrativos y de facturación perteneciente al dueño de la línea, se procede a realizar el corte del servicio de llamadas internacionales o nacionales salientes, luego de la respectiva autorización de la entidad regulatoria [14].

Este fraude puede generar pérdidas muy significativas a la entidad, en caso de ser víctima del hackeo de PBX, si no prevé este riesgo asegurando la terminal IP de su central para que ningún usuario ajeno pueda acceder libremente [14].

2.1.6. Fraude de roaming

Para el fraude por roaming existen algunas señales analizadas dentro del comportamiento de la red local y desde las operadoras en el extranjero que es donde se adquieren los chips con servicio roaming [14]:

- Servicio roaming solicitado para más de 10 líneas en el extranjero.
- Incremento de la cantidad de números comodín asignados a líneas “visitantes” (con servicio roaming activado).
- Llamadas en horarios inusuales y de larga duración originadas desde los números comodín.

- Demandas de delito Bypass, por parte de otras operadoras locales.

2.1.7. Falsa respuesta a llamada

Si al realizar un análisis del tráfico telefónico internacional entrante se encuentra una reducción significativa o atípica en la curva y luego de aplicar los procedimientos de detección usuales para Bypass, no se encuentra resultado de fraude, es probable que se trate de un fraude por FAS [14].

Para la detección de este fraude, la operadora o agencia de detección debe comprar las tarjetas que ofrecen servicios de tiempo aire hacia el Ecuador y realizar un análisis del ASR (Answer Seizure Ratio) y la calidad del servicio, si estos indicadores presentan valores muy bajos, existe una alta posibilidad de verse afectados por fraude de falsa respuesta a llamada [14].

Según el funcionario de la ARCOTEL, muy pocas operadoras en el país contemplan la posibilidad de enfrentarse ante este tipo de fraude. Para realizar el control del mismo la empresa debe reportar el carrier defraudador [14].

2.1.8. Fraude de suscripción

Para controlar este tipo de fraude es necesario que las operadoras tomen medidas sancionatorias para los distribuidores, puesto que éstos deben procurar que los datos de los clientes sean cuidadosamente corroborados, a fin de obtener información verídica del Estado crediticio y datos de contacto; se debe evitar la suscripción por parte de terceros, puesto que, esto también origina fraude por suplantación de identidad [14].

A continuación, en la tabla 3 se presenta una lista de “métodos de comunicación no autorizados” que la operadora OTECEL expide a sus

abonados en cada contrato de suscripción para protegerse legalmente contra este fraude [41]:

MÉTODOS DE COMUNICACIÓN NO AUTORIZADOS
Call back
Bypass
Reoriginamiento de llamadas
Tercer país
Reventa y/o comercialización de servicios sin autorización del operador
Uso y/o manipulación no autorizada de redes por parte del cliente a través de terceros
Alteración de cualquier equipo, sistema o dispositivo de acceso de tal forma que se modifique la medición del consumo de los servicios o se sustraiga su pago.
Acceso no autorizado a códigos de acceso o números de identificación personal.
Acceso a servicios suplementarios o a categorías de programación sin previa autorización del operador.
La interceptación de comunicaciones sin orden de autoridad competente; o cualquier modalidad similar o de uso ilegal de las redes y de fraude en su utilización; o cualquier otra forma de incumplimiento o violación de las disposiciones legales, reglamentarias o contractuales en materia de telecomunicaciones.
La instalación de Malware: software malicioso.
Smishing: Fraude por mensajes de texto.
El acceso no autorizado por medio de internet a servidores o servicios telefónicos (hardware o software) con el fin de vulnerar la seguridad de otros clientes.
Vishing: por medio de una llamada de VoIP y la ingeniería social engañar a personas para obtener información financiera o útil para la suplantación de identidad.

Tabla 3: Métodos de comunicación no autorizados por la operadora OTECEL a sus clientes [41].

2.1.9. Fraude interno

Actualmente las operadoras detectan el fraude interno a través de bitácoras de actividades y auditorías en todos los departamentos, realizan un continuo escaneo de las actividades realizadas diariamente y

cuando perciben una irregularidad en las actividades de un empleado, solicitan la respectiva explicación [42].

La protección de datos confidenciales tales como los códigos de las tarjetas prepago resulta prioritaria, por lo que hoy en día las operadoras prefieren delegar el tratamiento de esta información a una sola persona y ya no a todo un equipo de trabajo como solía ocurrir en años anteriores [42].

Para controlar la cantidad y valor de las recargas realizadas en las plataformas de prueba, los asesores cuentan con un código de identificación; de tal manera que toda transacción realizada por ellos debe ser respaldada por el respectivo código [42].

2.2. Sistemas de detección de fraude utilizados en el Ecuador

Es primordial que los sistemas antifraude que se deseen implementar sean adaptables a la infraestructura existente en las operadoras y red nacional, como también a los servicios ofertados y al desarrollo de la industria local e internacional [43]; es por ello, que cada país posee sistemas y técnicas de detección adaptadas para su respectivo entorno y de acuerdo a sus necesidades prioritarias en el tema de fraude en telefonía fija y móvil.

Según el Ing. Roberto Pérez de la ARCOTEL, existen 3 sistemas que permiten el combate efectivo al fraude en telefonía fija y móvil aplicados en las operadoras telefónicas del país, estos se encuentran indicados en el orden de prioridad o efectividad ante la detección [14]:

- Loop de llamadas
- Análisis de CDRs
- Perfilamiento

En esta sección se describirán a detalle cada uno de estos sistemas y procedimientos realizados para detectar el fraude en la telefonía fija y móvil.

2.2.1. Loop de Llamadas (Lazos Telefónicos de llamadas)

Este método de control de fraude consiste en realizar llamadas internacionales con el propósito de hallar irregularidades que sean indicadores potenciales de fraude y realizar un constante monitoreo a los canales y rutas de comunicación telefónica con el país [24].

Para desarrollar las pruebas se debe realizar llamadas telefónicas desde el extranjero y con una tarjeta telefónica pre pagada; en un principio, se enviaba a una persona al exterior para realizarlas pero debido al alto costo que esta metodología generaba y al avance tecnológico alcanzado, se logró automatizar este sistema que opera de la forma mostrada en la Figura 2.3 [14].

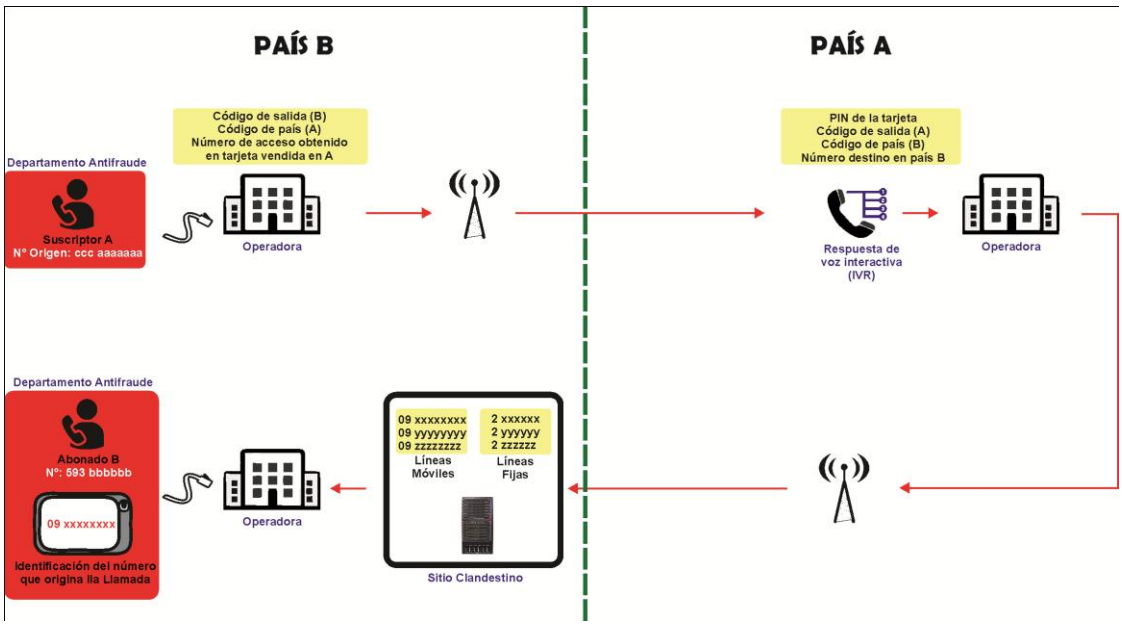


Figura 2.3: Diagrama del sistema Loop de llamadas automatizado

Los encargados de identificar el fraude adquieren las tarjetas pre pagadas fraudulentas como las mostradas en la Figura 2.4, las cuales normalmente promocionan el valor de la llamada internacional a un

menor precio que las tarjetas legales; esta adquisición se la realiza de forma masiva en línea [44].

Figura 2.4: Tarjetas pre pagadas para realizar llamadas internacionales [44].

Una vez adquiridas, el sistema antifraude se encarga de realizar una llamada, con las claves proporcionadas por las tarjetas (Número de acceso y PIN), hacia los terminales de prueba en el mismo país, el lazo se encuentra detallado en la Figura 2.3. Luego, el terminal fijo o móvil que se emula, recibirá una llamada que podrá mostrarse de tres maneras, si su ruta internacional es legal [14]:

- Código identificador de carrier
- Código internacional, código de país y número telefónico de donde se realiza la llamada
- Texto en pantalla “Desconocido”

En cambio, si la ruta de la llamada es ilegal, el número que se muestra en el identificador corresponde a una línea telefónica local, ya sea fija o celular [14].

Existen softwares que realizan estos procedimientos de forma automática, por medio del log de llamadas, se logra realizar una

recopilación de todas aquellas líneas ilícitas que se encuentran operando, es decir, aquellos carriers locales obtenidos a partir de una llamada internacional [14].

Una vez detectadas las miles de líneas fraudulentas, el software antifraude se encarga de generar un reporte detallado de las mismas haciendo que el tiempo de localización del sistema fraudulento se optimice y disminuya [14].

Un software muy utilizado, para implementar este método de lazo, se encuentra desarrollado en base a Asterisk, programa de software libre que permite desarrollar sistemas de comunicaciones, ya sean analógicos, digitales o VoIP. Un ejemplo de log de llamadas en dicho software se encuentra en la Figura 2.5.

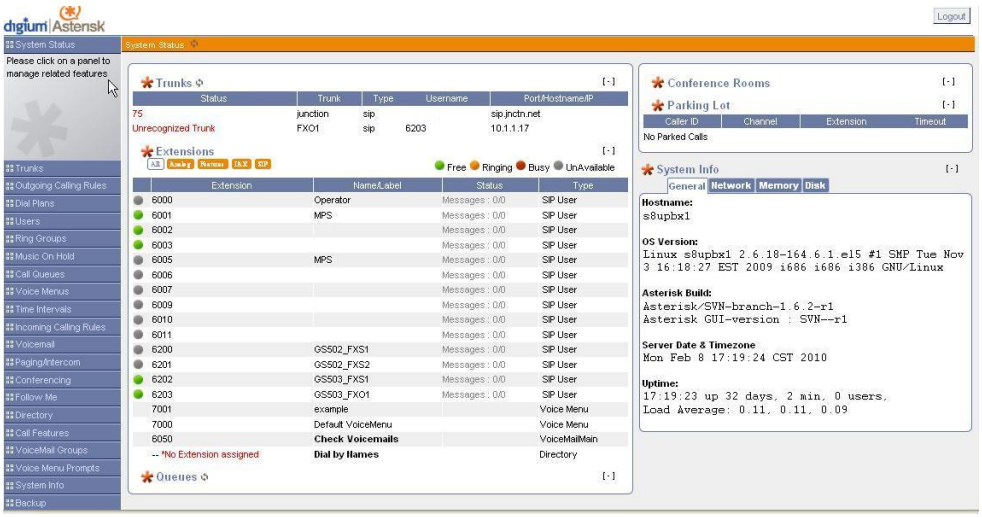


Figura 2.5: Log de llamadas en Asterisk [45].

Vale recalcar que actualmente existen varias empresas dedicadas a vender los software de detección para lograr identificar el fraude, estos proveedores solicitan el permiso necesario a las operadoras para acceder a la información de las centrales y así poder identificar de manera eficiente y masiva los números que cometen el acto ilegal [14].

El hardware que se utiliza para armar este sistema, está compuesto básicamente de tres componentes (Figura 2.6):

- Computador
- Conmutador
- Gateway

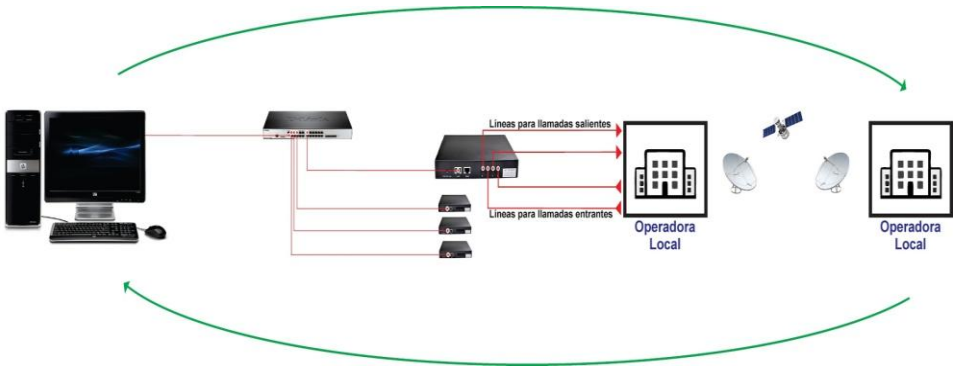


Figura 2.6: Sistema Loop de llamadas automatizado [14]

2.2.2. Análisis de CDRs Internacionales

Cuando un usuario realiza una llamada y ésta es completada exitosamente, la central almacena toda la información de dicho proceso en un registro de llamadas, generando CDRs por cada comunicación telefónica.

Un CDR (Figura 2.7), es un registro sobre las llamadas, que son generados automáticamente y analizados por computadora en distintos formatos. Estos reportes contienen información importante como el número de llamadas realizadas, la duración, el origen, destino y gasto de las mismas [46].

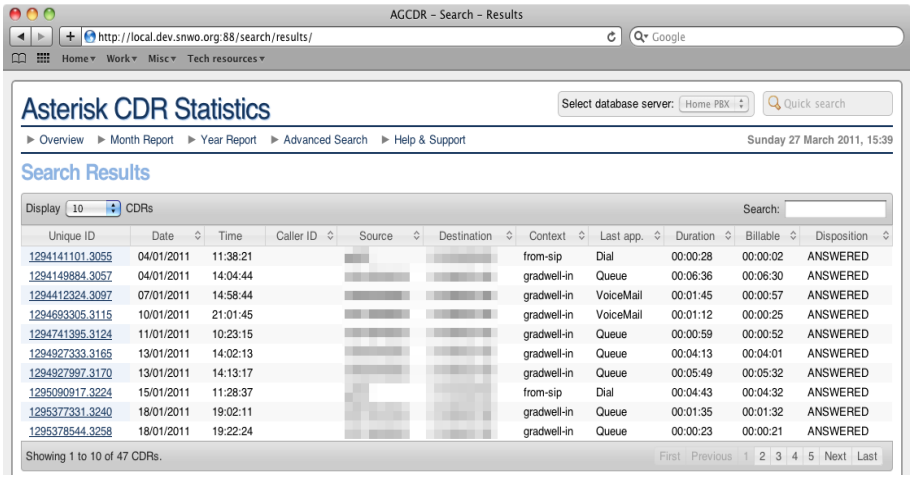


Figura 2.7: Call Detail Record [47]

Algunos consideran a los CDRs como una mina de oro, ya que en ellos casi siempre puede encontrarse la información que ayudará a determinar la existencia de los diferentes fraudes en telefonía fija y móvil, generalmente este método de detección nace gracias a la cooperación entre las operadoras locales y diversos carriers internacionales que se encargan de compartir sus CDRs de manera periódica, la clave para que el método sea efectivo radica en obtener ayuda del mayor número de carriers internacionales como sea posible (Figura 2.8) [14].

Según lo analizado previamente, se deduce que existe una anomalía cuando se observa un descenso abrupto en el tráfico de las llamadas internacionales entrantes en la red de una operadora local, por lo que cuando esto sucede, se recurre inmediatamente a estudiar el tráfico internacional generado por los diferentes carriers y con esta información se logra complementar el análisis de fraude que nos llevará a descubrir los posibles carriers internacionales cómplices de actividades ilícitas [14].

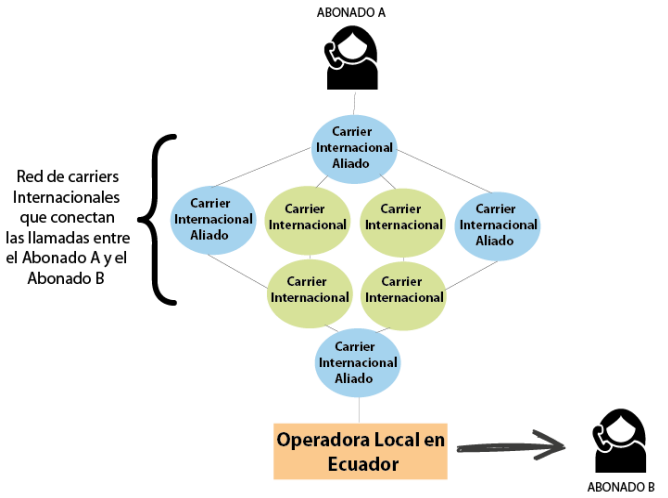


Figura 2.8: Análisis de CDRs Internacionales [14]

PROCEDIMIENTO PARA DETECTAR FRAUDE A TRAVÉS DE CDRS [14]

- Se establece una ventana de tiempo para efectuar el análisis entre CDRs de las diferentes operadoras locales y carriers internacionales.
- Se analizan todos los CDRs con tráfico internacional hacia Ecuador.
- Se comprueba que el tráfico generado en el extranjero haya terminado en el Ecuador de manera legal.
- Si existen CDRs diferenciales entre los registros de ambas partes (Figura 2.9), se concluye que existe un indicio de fraude.

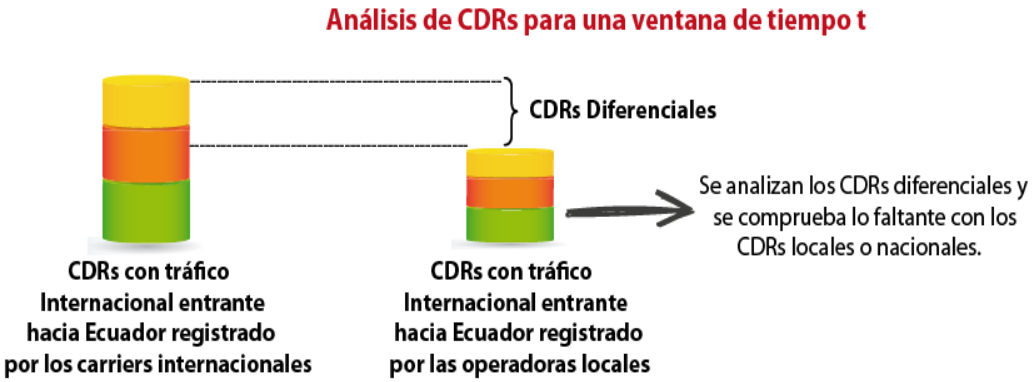


Figura 2.9: Análisis de CDRs Internacionales diferenciales [14]

2.2.3. Perfilamiento

Las operadoras telefónicas, usualmente, monitorean el tráfico total entrante y saliente de su red para poder detectar anomalías que reflejen un fraude. Por ejemplo, en la Figura 2.10 se muestra una curva del tráfico telefónico total; es normal observar ciertas oscilaciones entre valores que no se reflejan como significativos, pero ya representa una irregularidad el pico encontrado en el año 1998; frente a este tipo de anomalías, las empresas deben tomar medidas para identificar si se trata de un acto ilícito y localizar a la línea responsable para poder bloquearla y evitar más pérdidas; para responder a estas interrogantes se procede a utilizar el método de perfilamiento de usuario.

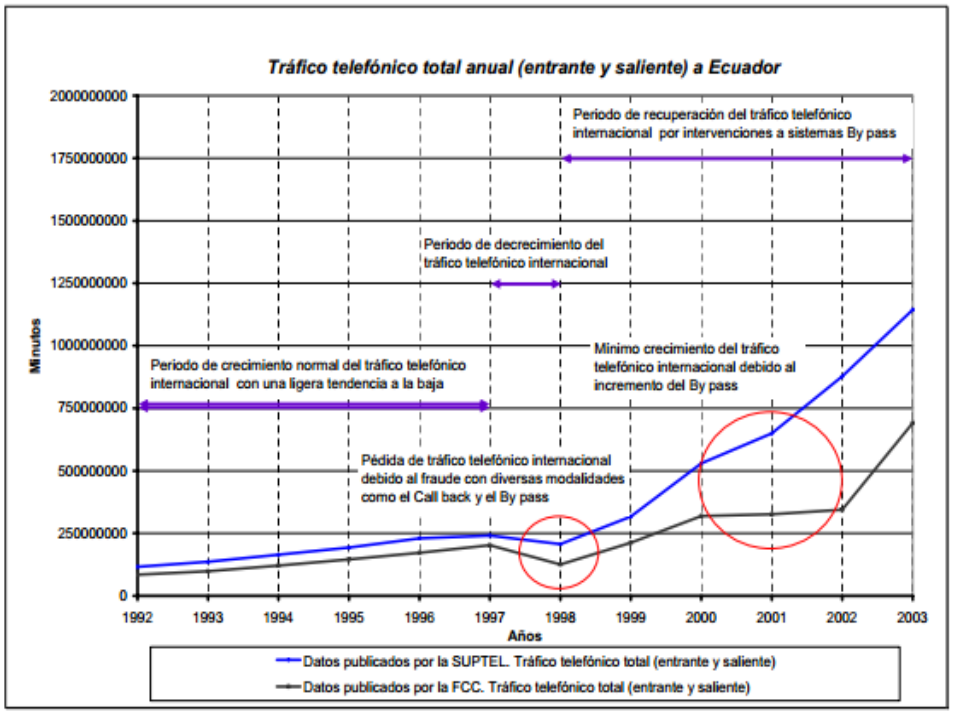


Figura 2.10: Tráfico telefónico total (entrante y saliente) [16]

El Perfilamiento permite percibir las actividades inusuales en el comportamiento o perfil telefónico de los usuarios; el sistema recibe y actualiza la información de las líneas telefónicas en tiempo real, así se generan curvas de tráfico de acuerdo a parámetros establecidos, ya sea por el dueño del software o programador de la operadora, entre estos indicadores tenemos los minutos de llamadas a larga distancia, horario de llamadas, actividad (sólo genera llamadas o sólo las recibe), etc [14].

La información se la obtiene de los CDRs y el sistema se encarga de analizar la información; el perfilamiento por tráfico telefónico muestra todas las líneas telefónicas que cumplen con ciertos parámetros generales de fraude o específicos por tipos de fraude.

Por ejemplo, el software muestra los números telefónicos que generan llamadas al extranjero por un tiempo prolongado, de los CDRs se puede obtener una cantidad muy grande de líneas con estas características, pero al aumentar las variables, como aquellos abonados que no reciben

llamadas, ciertos números se van descartando hasta llegar a obtener sólo las líneas telefónicas que con mayor probabilidad están siendo usadas para fraude [14].

Luego de tener esta información, ya más reducida y puntual, se puede realizar un perfilamiento por usuario para así resaltar las características que los convierte en defraudadores. Este sistema se basa en técnicas inteligentes como la minería de datos, redes neuronales, entre otros [14].

El software ayuda al modelamiento de datos y emite alertas de fraude, pero las operadoras telefónicas cuentan con personal capacitado y especializado en notar las irregularidades en las curvas, proporcionadas por el programa, de manera eficaz y rápida para no permitir mayores pérdidas [14].

El hardware que se utiliza para este sistema de perfilamiento es muy sencillo, pues solo lo compone un computador conectado a la red para poder tomar la información de los CDRs de la operadora, para su posterior análisis [14].

Algunas herramientas de análisis son [16]:

- Tablas Dinámicas
- Macros
- Plataformas adquiridas de empresas dedicadas a la detección de fraude.

2.3. Diseño de sistema para la Detección de Fraude en telefonía fija y móvil en Ecuador

Durante la entrevista realizada a un funcionario del Departamento de Aseguramiento de Ingresos de CONECEL el día 29 de Diciembre de 2015, salió a relucir el fraude OTT como una metodología que no se había visto antes en el país y declaró que, a pesar de que se constató la existencia de este fraude en el país, las operadoras aún no contaban con las plataformas que adviertan dicho ilícito.

Con el objetivo de investigar más a fondo las actuales tendencias de fraude y sistemas de control, el 12 de Enero de 2016 se llevó a cabo una reunión con el Ing. Roberto Pérez, funcionario de la ARCOTEL en la ciudad de Quito; quien corroboró el auge del fraude por medio de aplicaciones OTT dentro del Ecuador, además de introducir un nuevo caso ilícito producto del uso de aplicaciones VoIP para realizar Bypass.

Posteriormente, gracias a la autorización otorgada por la operadora CNT EP, se realizó una visita técnica guiada a la Jefatura de Prevención de Fraude en la ciudad de Guayaquil, donde se identificaron las plataformas antifraude utilizadas en la actualidad, lo cual permitió tener una visión de los componentes con los que se puede trabajar para diseñar los sistemas idóneos para las operadoras.

Finalmente, como resultado de todas estas entrevistas, se pudo constatar que los sistemas empleados actualmente no pueden detectar los fraudes por OTT ni Bypass desde smartphone, descritos en la sección 1.4, por lo que a través de este proyecto integrador se aportará con el diseño de dos sistemas basados en la metodología del loop de llamadas, analizada previamente, complementando así las actuales estructuras antifraude que tienen las operadoras, para así lograr la detección oportuna de estas nuevas tendencias de fraude.

Resulta importante clarificar que los diseños se han dividido según el tipo de fraude, el primero está orientado a detectar el Bypass desde smartphone, que afecta a los proveedores de telefonía fija; mientras que el segundo detectará el fraude por OTT, principal amenaza para los servicios de telefonía móvil.

2.3.1. Sistema de detección de fraude Bypass producido desde smartphones.

El Bypass desde smartphone representa una amenaza que con el pasar de los años se incrementará en Latinoamérica e incluso podría convertirse en uno de los delitos más practicados a nivel mundial, por lo que resulta necesario contar con el equipo necesario para contrarrestar los efectos negativos que este delito ocasiona.

El diseño propuesto en este proyecto integrador (Figura 2.11) pretende convertirse en un complemento al sistema de loop de llamadas analizado previamente, los elementos de hardware utilizados permitirán obtener nuevos indicadores que determinarán la existencia de Bypass producido desde smartphone; reforzando así las plataformas antifraude actuales.

Figura 2.11: Sistema de detección de fraude Bypass por Smartphone

El diseño, tal como se muestra en la Figura 2.11 se divide en 4 etapas explicadas a continuación:

Para empezar, se tiene un computador con múltiples cuentas Skype previamente recargadas, todas ellas creadas a partir de diferentes usuarios y contraseñas; que generan llamadas a números de telefonía fija en Ecuador de forma automática y consecutiva.

Para lograr esto se ha creado un script (Figura 2.12), que al ingresarlo en el cmd (Command Prompt) del computador, realiza las llamadas Skype sin necesitar la presencia de un operador (Figura 2.13).

```
C:\>cd Program Files (x86)\Skype\Phone\
C:\Program Files (x86)\Skype\Phone>skype.exe /secondary
C:\Program Files (x86)\Skype\Phone>
C:\Program Files (x86)\Skype\Phone>Skype.exe /callto:vix
```

Figura 2.12: Script para realizar llamadas automáticas

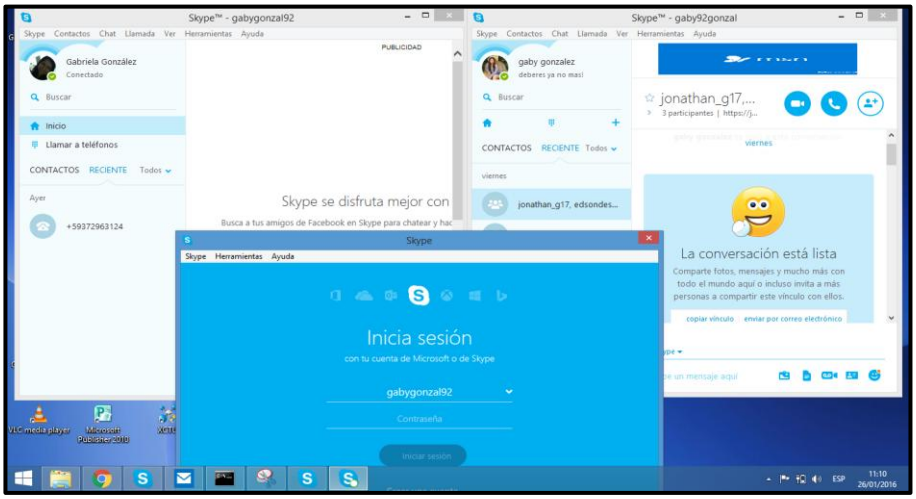


Figura 2.13: Múltiples usuarios Skype listos para realizar llamadas

Para el caso de la Figura 2.14, *vix* es el usuario del contacto en Skype a quién se quiere llamar. Al tratarse de un teléfono fijo se deberá ingresar el código de área del país destino seguido del número local. Para ambos casos aparecerá un mensaje de confirmación como el de a continuación, el mismo que debe ser aceptado (Figura 2.14).

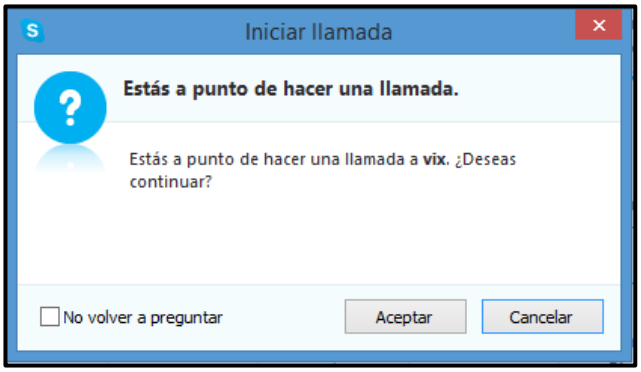


Figura 2.14: Mensaje de confirmación de llamada en Skype

Luego de haber generado la llamada Skype hacia el destino fijo en Ecuador, el sistema procede a monitorear el tráfico generado con el objetivo de documentar la hora y destinos alcanzados mediante las llamadas. Para esto se utiliza Wireshark (Figura 2.15), un analizador de protocolos de red muy utilizado en la actualidad.

Se identifica puertos que Skype utiliza para generar tráfico UDP en el computador (Figura 2.16) y se filtra el tráfico con el fin de observar todo lo que ocurre exclusivamente en ese puerto.

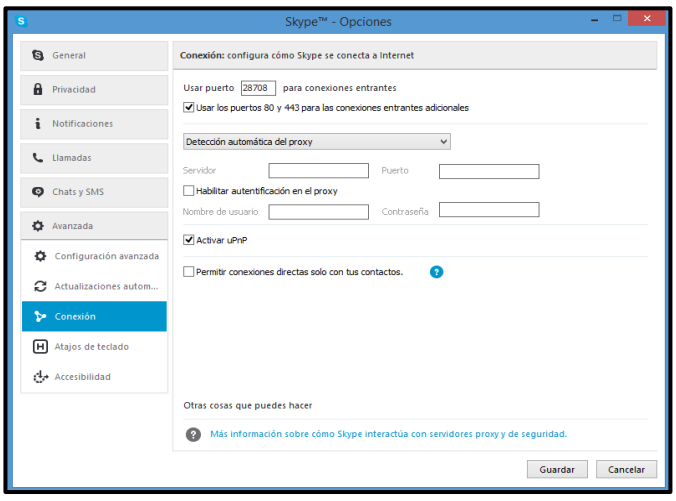


Figura 2.15: Identificación del puerto utilizado para cursar el tráfico Skype

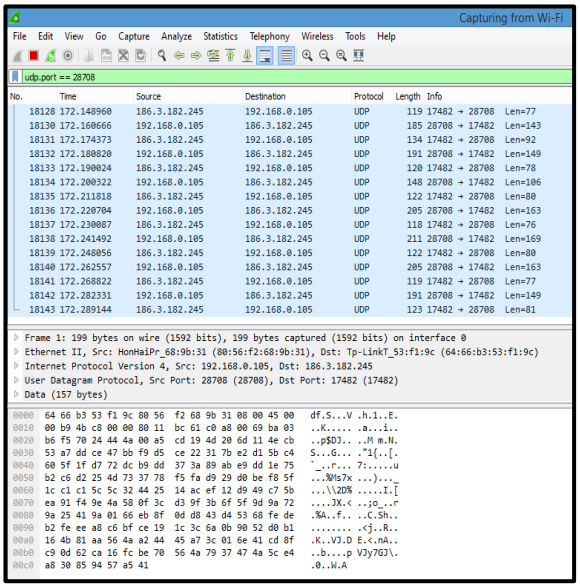


Figura 2.16: Análisis en Wireshark del tráfico Skype generado a través del puerto identificado

Tras realizar la llamada en Skype, el sistema recibe la llamada por medio de una línea telefónica conectada al computador, vale la pena recalcar que con el objetivo de no ser identificados por los defraudadores, el sistema realiza llamadas a diferentes ciudades del país, transfiriendo todo el tráfico a la línea del sistema.

Para conectar la línea telefónica en el sistema propuesto se sugiere el uso de una tarjeta analógica Digium de 4 puertos modelo TDM404 (Figura 2.17) , ya que permite la recepción de tráfico VoIP en nuestra línea fija y es compatible con plataformas de configuración de PBXs como asterisk y Trixbox. [42]

Figura 2.17: Tarjeta telefónica analógica Digium TDM404 [48]

La mayoría de la operadoras de telefonía fija y móvil utilizan softwares antifraude encargados de administrar el loop de llamadas, uno de los más usados es *Taurus,* este proporciona un registro completo de los números sospechosos identificados durante el transcurso de las llamadas [15]. El diseño propuesto en este proyecto integrador utilizará los registros proporcionados por Taurus para compararlos con el tráfico identificado en Skype y encontrar las irregularidades típicas del fraude Bypass.

2.3.2. Fraude OTT

Se han detectado casos de Fraude por OTT en todo el mundo [34], esta modalidad es un gran ejemplo de la equivalente evolución entre el fraude y la tecnología.

Si al realizar un análisis del tráfico telefónico o comparar las llamadas registradas por el operador internacional y los registros de llamadas del operador nacional, se descubre una inconsistencia de registros que no se explica con ninguno de los fraudes descritos anteriormente, se concluye que se trata de un fraude, ya sea FAS u OTT.

Para descartar el fraude por FAS se debe comparar con las curvas de tráfico nacional para poder encontrar coincidencias de variables como hora, duración de la llamada, fecha, entre otros, de modo que si no se encuentra registro alguno, existiría mayor certeza de que se trata de fraude OTT.

Como se lo mencionó anteriormente, el sistema que se diseñará se basa en el método del loop de llamadas, de modo que para identificar este tipo de fraude el diseño debe cumplir con las siguientes funciones:

- Realizar llamadas desde plataforma PSTN (Public Switched Telephone Network) o GSM.
- Recibir llamadas GSM.
- Recibir llamadas en una aplicación OTT.

El funcionamiento del sistema diseñado consiste en generar una llamada desde el Ecuador hacia el extranjero, para luego generar tráfico entrante al Ecuador nuevamente y así poder identificar la ruta que genera la llamada; la diferencia con los sistemas implementados actualmente, radica en que el software debe contar con la aplicación o conjunto de aplicaciones que estarían involucradas en este tipo de fraude.

El diseño propuesto en este proyecto integrador se muestra en la Figura 2.18.

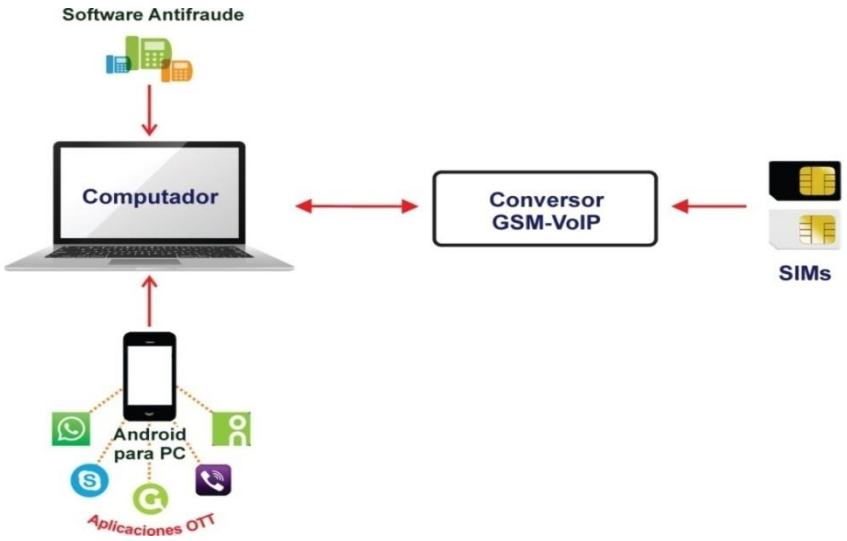


Figura 2.18: Topología del diseño de detección para Fraude OTT

El sistema está compuesto por los siguientes componentes:

- Hardware:
  - SIMs
  - Conversor GSM - VoIP
  - Computador
- Software:
  - Software Antifraude
  - Emulador Android
    - Aplicaciones OTT instaladas

A continuación se describe la operatividad de los elementos y las características de los mismos.

CONVERSOR GSM-VOIP

Para identificar si la llamada entrante es por la ruta legal (GSM), es necesario contar con un equipo que permita recibir dichas llamadas para luego direccionarlas a un computador que las registre para la verificación oportuna.

Debido a que este fraude produce mayor impacto en la telefonía móvil, se debe poder recibir y realizar llamadas a números móviles, para ello se tiene que establecer una conexión entre la red GSM y nuestra red por medio de la tecnología VoIP.

Existen muchos dispositivos o combinación de ellos, que permiten realizar la administración de las llamadas dentro de la red GSM, enviar y recibir mensajes, entre otras características, a continuación se mencionan los equipos que se adaptan al diseño propuesto:

- Módulos GSM (Figura 2.19): su principal beneficio es la facilidad de instalación, puesto que la conexión y alimentación dependen de los recursos de la computadora donde se realice la instalación.

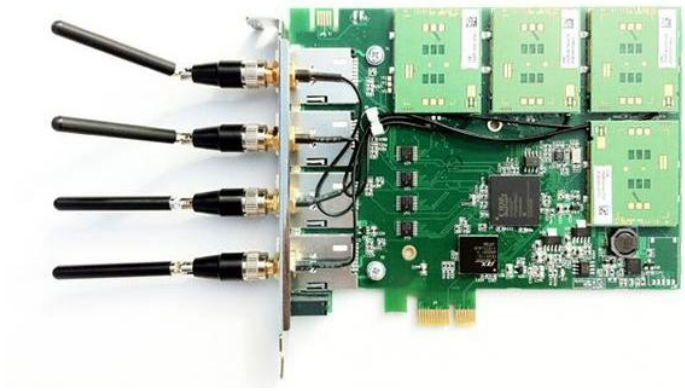


Figura 2.19: Tarjeta GSM SANGOMA W400. [49]

- Bases celulares (Figura 2.20): Este componente resulta más fácil de encontrar en el mercado, pero se debe tomar en cuenta sus características técnicas, a fin de que permitan la recepción de mensajes SMS para simplificar la configuración de las aplicaciones OTT, y el número de entradas SIM o bases celulares a adquirir, debido a que se necesita colocar mínimo 2 líneas celulares para las respectivas llamadas entrantes y salientes.

Figura 2.20: Base celular GSM GFX11 de 1 puerto SIM. [50]

- Gateway GSM-VoIP (Figura 2.21): En el mercado existen varios modelos y marcas de estos tipos de gateways, desde equipos con un solo puerto para insertar la tarjeta SIM, hasta aquellos que poseen más de 32 canales GSM; su ventaja radica en la escalabilidad que le puede dar al sistema.

Figura 2.21: Gateway OpenVox VS-GW1600-20G. [51]

EMULADOR ANDROID

Para poder verificar si las llamadas ingresan al país por medio de una ruta legal se debe confirmar que las mismas sean recibidas vía GSM, es decir por las SIMs colocadas en el gateway a las que estamos llamando; en caso de que la comunicación no finalice por el medio habitual, se debe tener activa la aplicación que se examinará como medio de fraude para constatar este hecho y poder realizar los informes pertinentes.

En este proyecto se va a contemplar el escenario de fraude mediante la aplicación Viber (Sección 1.4.8).

Existe la posibilidad de instalar la aplicación en la computadora que se va a utilizar, pero Viber restringe su uso si el usuario no registró previamente una cuenta desde su teléfono inteligente (Figura 2.22)

Figura 2 22: Pantalla de activación de Viber en el escritorio

La alternativa más viable es disponer de un emulador de sistema Android, que dará la facilidad de instalar la aplicación y aprobar la debida autenticación como si se tratase de un teléfono inteligente.

Para este escenario se utilizará el emulador BlueStacks, donde se debe instalar la aplicación Viber y crear una cuenta, autenticándola con el mensaje SMS que llega a la línea vinculada con el computador.

Las plataformas de detección, que actualmente utilizan las operadoras telefónicas, no cuentan con las herramientas para generar notificaciones en el caso de que reciban llamadas hacia una aplicación.

Se han desarrollado programas que permiten tener control sobre los usos de los dispositivos, internet y aplicaciones, de modo que si hacemos uso de estas herramientas, obtendremos una forma sencilla de detectar si recibimos llamadas por medio de la ruta ilegal.

Para usar Qustodio, se la debe instalar en el dispositivo que se va a controlar, para ello se creó una cuenta empresarial y se descargó la aplicación en el smartphone emulado (Figura 2.23).

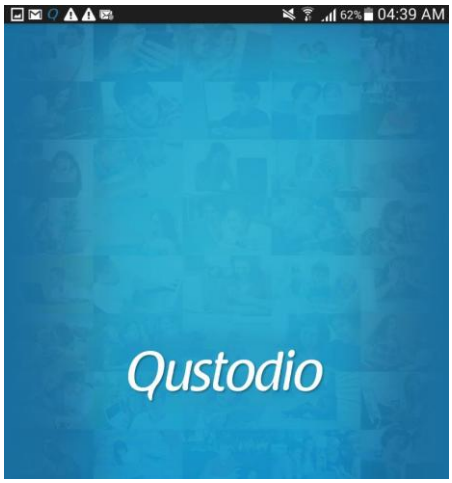


Figura 2.23: Aplicación Qustodio instalada en Smartphone.

Mediante la página web del proveedor del servicio, se puede obtener los registros de las actividades del smartphone, donde se debe focalizar en las actividades sociales entre usuarios de Viber y otras aplicaciones que se quieran analizar. Por ejemplo, en la Figura 2.24 se muestra la cronología de las aplicaciones utilizadas por el usuario respectivo y el tiempo de duración en dicha aplicación.

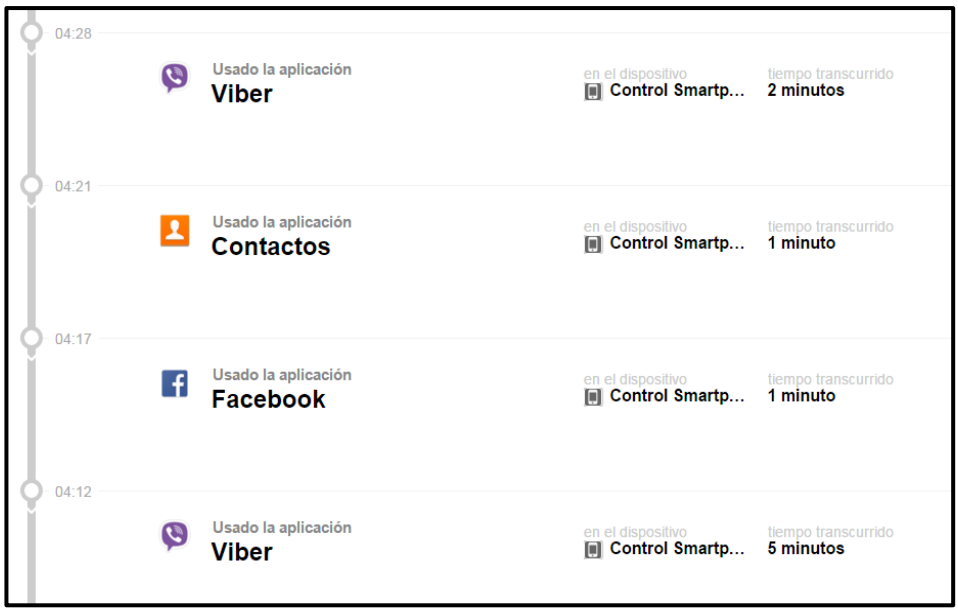


Figura 2.24: Cronología de la actividad para un usuario

Las facilidades que brindan las líneas telefónicas y dispositivos utilizados para la detección es la exclusividad, puesto que si se realiza el loop de llamadas y se llega a detectar actividad en el dispositivo, se puede tener la seguridad de que se trata de fraude, puesto que dicho sistema no debe registrar ningún tipo de actividad.

En el caso de Qustodio, se puede ajustar el periodo de las notificaciones entre las opciones mostradas en la Figura 2.25.

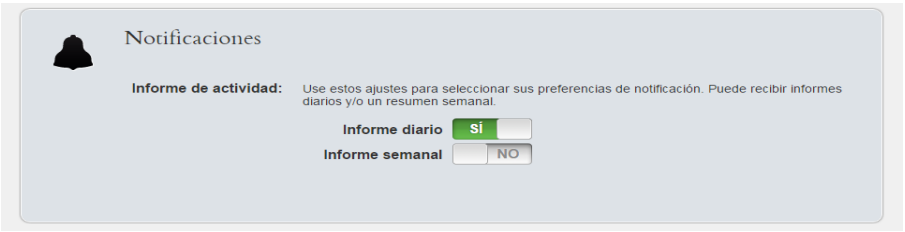


Figura 2.25: Configuración de notificación de Qustodio

SOFTWARE ANTIFRAUDE

La plataforma debe ser cargada previamente con información de las tarjetas que se compran en el extranjero para poder realizar las llamadas; como en un proceso de detección de Bypass normal, el robot registra el identificador de la llamada, que puede ser de un carrier o de una línea nacional [15].

Cuando se produce fraude OTT la llamada no es recibida en el software, por lo cual marcará un error; dependiendo de la configuración del sistema, el proceso se detendrá automáticamente para que el técnico pueda revisar si hay algún problema de enlace u otro factor que no permita recibir la llamada por el medio convencional; este hecho alertará a los funcionarios quienes, con la ayuda del programa mencionado anteriormente, tendrán información suficiente para determinar si se trata de fraude o no.

Si se desea obtener más pruebas que confirmen la ejecución del fraude, se puede proceder a analizar el tráfico cursado por los puertos y así realizar un estudio de protocolo, IPs, fecha y hora del suceso irregular.

CAPÍTULO 3

3. RESULTADOS Y BENEFICIOS

La investigación de los diferentes fraudes que afectan a la telefonía fija y móvil nos advierten de los peligros inminentes que corren las operadoras que prestan estos servicios en el Ecuador, la evolución de los métodos para cometer fraude no se detiene, y tampoco debe hacerlo la evolución de los sistemas de detección basados en nueva tecnología.

3.1. Resultados

Se considera que la implementación de los diseños propuestos en este proyecto integrador producirá, como resultado, un refuerzo significativo de los actuales sistemas antifraude, que permitirá a las operadoras percibir aquellas actividades ilícitas de las cuales las plataformas instaladas actualmente aún no logran percatarse.

El resultado de la detección eficiente de los fraudes por Bypass desde smartphones y OTT es evitar pérdidas considerables de dinero para las operadoras y el Estado; mejorando de esta manera la economía del país y situando a Ecuador como un ejemplo de los países que previenen eficientemente el fraude producido en la telefonía fija y móvil.

La implementación de los sistemas planteados permitirá al operador determinar eficientemente el tipo de fraude cometido. Actualmente, las operadoras pueden llegar a determinar el tipo de fraude ejecutado a partir del análisis de los diferentes criterios de detección que sus sistemas le proveen, pero cuando el fraude es producido por Bypass desde Smartphone u OTT los criterios no son suficientes, lo que genera confusión e incertidumbre.

3.1.1. Análisis económico de la implementación

Los sistemas diseñados en este proyecto integrador están basados en el método de detección “Loop de llamadas”, que actualmente actúa en todas las operadoras de telefonía fija y móvil. Para el loop de llamadas,

el software antifraude que se emplea puede ser adquirido (a precios muy altos) o desarrollado (después de mucho tiempo) por la operadora; muchas empresas de telecomunicaciones que tienen sus sistemas de detección ya cuentan con este programa.

Las aplicaciones y la mayoría de programas adicionales utilizados en los diseños previamente propuestos son creados a base de softwares libres, por lo cual las operadoras no requieren de una inversión adicional; además los equipos que operan en los sistemas de detección actuales no deberán ser reemplazados permitiendo el ahorro de recursos en las empresas. Existe la alternativa de usar programas pagados que permitan el análisis de tráfico y notificaciones de uso de recursos en los móviles, pero su efectividad dependerá del presupuesto asignado por la empresa.

En la tabla 4 se muestra la inversión inicial en equipos para el fraude Bypass desde smartphone, que comprende tan sólo de un computador, donde se instalarán los programas utilizados para la detección y una tarjeta analógica donde se configurarán las líneas de telefonía fija.

ELEMENTO	PRECIO POR UNIDAD	TOTAL
Tarjeta telefónica analógica Digium TDM404 de 4 puertos	$90,46	$90,46
Computadora	$500	$500

Tabla 4: Precios de los recursos para sistema de detección de fraude desde smartphone

En la tabla 5 se muestra la inversión inicial en equipos para el fraude OTT. Este análisis se lo realiza para un sistema básico que conste de dos líneas móviles (una receptora - una transmisora), el modelo es escalable y dependerá de los recursos que se utilizan en la conversión VoIP-GSM.

ELEMENTO	PRECIO POR UNIDAD	TOTAL
Chips GMS	$2	$4
Módulo GSM	$60	$120
Computadora	$500	$500

Tabla 5: Precios de los recursos para sistema de detección de fraude OTT

Cabe recalcar que los costos de inversión presentados representan una inversión mínima en comparación con lo que debería invertirse si la operadora decide comprar los sistemas ofrecidos por compañías antifraude extranjeras. Además para poder implementarlos posiblemente tendrán que migrar de tecnología lo que implicaría invertir más dinero de lo propuesto en el presupuesto anual.

3.2. Beneficios

A continuación se presentan los distintos beneficios que genera la implementación de los sistemas diseñados en este proyecto, como se mencionó anteriormente las operadoras de telefonía fija y móvil aún no logran percibir el perjuicio que ocasionan el fraude OTT y Bypass desde smartphone pues no cuentan con un sistema que les permita detectarlos.

Los sistemas propuestos tienen el objetivo de complementar el trabajo que han venido realizando las operadoras en mejorar sus sistemas, es decir, cada uno de los diseños brindan la facilidad de ajustarse a los recursos técnicos que posee la empresa sin necesidad de migrar la tecnología o de adquirir nuevos equipos costosos.

3.2.1. Beneficio de la técnica de detección utilizada

El loop de llamadas es la técnica más usada por las operadoras y empresas dedicadas a la detección de fraude en el sector de las telecomunicaciones, además permite el monitoreo en tiempo real del tráfico generado por los dispositivos finales asignados y que está cursando por la red de dicha operadora.

Los sistemas propuestos se basan en esta técnica, lo que permitirá que el proceso de detección sea más eficiente debido a que las alertas se generan inmediatamente después de haber sido cumplidos todos los parámetros seteados, lo que con otros métodos puede durar días.

Al implementar los sistemas planteados, el método del loop de llamadas quedará complementado, lo que le posibilitará la identificación de los respectivos fraudes estudiados, además su gestión no resultará nueva para las compañías de telecomunicaciones, más bien simplificará la familiarización del personal con el mismo.

Como se mencionó en el capítulo 2, el sistema del loop de llamadas es automatizado, lo que permite realizar las pruebas tanto en horarios de oficina, como horarios nocturnos los 7 días de la semana, permitiendo una detección más efectiva.

3.2.2. Factibilidad de la implementación

El diseño propuesto utiliza muchos de los recursos con los que las operadoras actualmente trabajan, lo que facilitará la implementación de estos sistemas y reducirá la inversión en equipos tecnológicos, por lo cual no habrá necesidad de migrar de tecnología o invertir en una plataforma antifraude distinta.

El sistema está desarrollado a partir de software y aplicaciones libres, lo que le permitirá a las operadoras ahorrar dinero.

La compañía telefónica ya debe contar con los módulos telefónicos analógicos o GSM necesarios para convertir las llamadas analógicas/GSM en VoIP y viceversa, computadoras, acceso a internet, líneas telefónicas o chips GSM y tarjetas telefónicas de los diferentes proveedores internacionales; la versatilidad del sistema permite hacer uso de cualquier medio electrónico que permita realizar las funciones requeridas. Además, tienen acceso a los programas utilizados para detectar los fraudes más comunes y los que les permiten analizar el tráfico que cursa por la red, estas herramientas son costosas pero si se las adaptan de la forma sugerida en la sección 2.3, no representará una inversión significativa.

3.2.3. Escalabilidad

Los procedimientos y equipos para cometer fraude han ido evolucionando de forma que usan estrategias para evadir las técnicas de detección, incluso hay compañías que se dedican a vender estos sistemas, donde aseguran soluciones innovadoras de rotación de tarjetas SIM, migración de líneas telefónicas, entre otras, para así evitar el bloqueo de tarjetas SIM, localización de Simbox, etc.

Ante estas posibilidades, los modelos planteados se diseñaron de tal forma que sean escalables y permitan alternar entre los números que generan la llamada y aquellos que las reciben para así evitar ser descubiertos por los defraudadores.

3.2.4. Plataforma anti Baneo

Tras haber realizado la visita a CNT EP percibimos que el software utilizado actualmente realiza llamadas desde Skype secuenciales de 1 minuto de duración y desde un mismo usuario; esto ocasiona una desventaja considerable, pues los defraudadores notan la irregularidad

que este usuario genera en sus redes provocando el bloqueo o baneo del mismo lo que dificulta aún más la detección.

Un beneficio importante es que los sistemas diseñados podrían llegar a realizar múltiples llamadas desde usuarios diferentes, todo esto con gran escalabilidad, dificultando así la detección de los mismos en la red de los defraudadores; por ejemplo, las llamadas se realizan una después de otra con diferentes usuarios Skype y a diferentes destinos del país, cada una con una duración de aproximadamente 1 minuto.

3.2.5. Beneficios para la operadora, usuarios y Estado ecuatoriano

En este estudio, se llegó a inferir que los fraudes, en general, afectan tanto a las operadoras, como a los usuarios y al Estado, por lo cual llegar a mitigar estos nuevos actos ilícitos se traduce en beneficio para todos los agentes mencionados.

BENEFICIOS PARA LA OPERADORA

El Bypass por smartphones y fraude por OTT son temas que muchos operadores encuentran difícil de identificar y más aún, difícil de contrarrestar, contar con un medio de control permitirá a las operadoras medir el grado de afectación y tomar las decisiones correctas para asegurar los ingresos de sus empresas, ya sea a corto, mediano o largo plazo, puesto que estos fraudes representan un problema potencial.

El monitoreo que nos permiten realizar los sistemas propuestos, ayudarán a las compañías de telecomunicaciones a educar a los legisladores sobre estas nuevas estrategias de fraude y así entablar contribuciones conjuntas para encontrar soluciones a dichos ilícitos.

La fácil implementación que los sistemas diseñados requieren beneficia económicamente a la operadora, pues utilizarán los mismos equipos y software de detección, evitando inversiones significativas.

Gracias a que los sistemas planteados utilizan recursos de software libre, la operadora no tendrá que pagar por licencias anuales para poder utilizarlos, evitando así la inversión en software.

BENEFICIOS PARA LOS USUARIOS

Los tipos de fraudes, que se busca detectar con el diseño de estos sistemas, perjudican al usuario en la calidad del servicio.

Para el caso de fraude por OTT, el usuario se perjudica porque consume sus datos al recibir una llamada que debió ser finalizada en la red GSM sin costo; mientras que para el Bypass producido desde smartphone el usuario se ve afectado al acreditar su cuenta Skype para realizar llamadas a teléfonos de telefonía fija en Ecuador, pero estas llamadas nunca se realizan de modo legal.

Por esta razón, un gran beneficio que ofrece la implementación de estos sistemas propuestos sería el poder medir el grado de perjuicio de estas actividades ilícitas en nuestro medio, lo que permitirá crear programas que eduquen o adviertan a los usuarios de estos métodos de finalización de llamadas, que en muchas ocasiones sólo se traducen como beneficio para los entes fraudulentos.

BENEFICIOS PARA EL ESTADO

Es importante que los organismos reguladores estén atentos al tráfico internacional entrante y cursante en el país, esto facultará al Estado para realizar inversiones y toma de decisiones en cuanto a los avances tecnológicos en el área de telecomunicaciones y detección de fraudes en la misma.

Al poder percatarse del perjuicio que representan los fraudes por Bypass y OTT a los ingresos de las empresas, el gobierno notará la afectación económica por no percibir los impuestos que le corresponden.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Tras haber realizado este proyecto integrador podemos concluir lo siguiente:

1. Las técnicas fraudulentas en el área de las telecomunicaciones han ido evolucionando de tal forma que los sistemas de detección y control se han visto obligados a desarrollarse a la par.
2. La detección del fraude en los sistemas de telefonía fija y móvil en el Ecuador se ha logrado gracias a la cooperación que ARCOTEL mantiene con las distintas operadoras telefónicas al compartir sus registros periódicamente y al gestionar los casos presentados ante la fiscalía de manera oportuna; sin embargo, estas medidas resultan ineficientes para detectar las nuevas modalidades de fraude, como las expuestas en este proyecto integrador.
3. Las acciones ilícitas en la telefonía generan pérdidas y afectan tanto a las operadoras como a los usuarios y al Estado.
4. La creciente popularidad de las aplicaciones OTT ha sido utilizada por los defraudadores para aprovecharse de las mismas con el fin de obtener beneficios económicos afectando la calidad de las llamadas y ocasionando otros perjuicios.
5. El riesgo a sufrir pérdidas económicas debido al Bypass desde smartphones y fraude por OTT es inminente, por lo que en un futuro próximo, el Estado ecuatoriano podría sufrir repercusiones económicas igual de graves que cuando surgieron los primeros casos de Bypass en nuestro país.

Recomendaciones

El fraude en los sistemas de telefonía fija y móvil debe ser controlado óptimamente, por lo cual, luego de haber realizado las investigaciones pertinentes se debería tomar en cuenta lo siguiente:

1. Es recomendable que las operadoras implementen cuanto antes los sistemas presentados en este proyecto integrador, pues mejorará la eficiencia en la detección de los fraudes evitando pérdidas significativas de dinero no solo a las operadoras de telefonía fija y móvil sino al Estado y a los abonados.
2. Las empresas de telecomunicaciones deberían estudiar y mantenerse al tanto de los nuevos modelos de negocios ilícitos que amenazan los ingresos de las operadoras y por consiguiente del Estado ecuatoriano.
3. Las operadoras y empresas dedicadas a la detección del fraude en el sector de las telecomunicaciones deberían desarrollar estrategias con el fin de desalentar el crecimiento del Bypass desde smartphones y fraude OTT.
4. El gobierno por medio de los organismos reguladores, debería ayudar a crear soluciones o medidas que permitan minimizar los efectos que estos nuevos tipos de fraude ocasionan.
5. Entre las estrategias que las empresas de telecomunicaciones diseñen contra el Bypass desde smartphone y fraude OTT, se debe tomar en cuenta la necesidad de educar a los usuarios sobre las consecuencias de estos actos ilícitos y su afectación.

BIBLIOGRAFÍA

[1] Unión Internacional de Telecomunicaciones, “Key ICT indicators for developed and developing countries and the world (totals and penetration rates)”, 2015.

[2] M. Castro. (2015,May). Las operadoras de telefonía podrán bloquear llamadas fraudulentas. ABC [Online]. Disponible en: http://www.abc.es/sociedad/20150514/abci-telefonia-fraude-llamadas-201505132033.html

[3] GSMA. (2012, Mayo 20). Celulares robados en Latinoamérica: el ejemplo de Costa Rica y la necesidad de coordinación entre operadoras [Online]. Disponible en: http://www.gsma.com/latinamerica/es/celulares-robados-en-latinoamerica-el-ejemplo-de-costa-rica-y-la-necesidad-de-coordinacion-entre-operadoras

[4] Communication fraud control association, “Global Fraud Loss Survey”, 2015.

[5] C. M. Gallardo, “Análisis de estrategias para control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las empresas de telecomunicaciones”, Tesis de pregrado, escuela de Ing., Escuela politécnica nacional, Quito, Ecuador, 2006.

[6] ARCOTEL. Servicio de Telefonía Fija [Online]. Disponible en: http://controlenlinea.ARCOTEL.gob.ec/wps/portal/informacion/informaciontecnica/telefoniafija/

[7] Agencia de regulación y control de las telecomunicaciones, “Densidad de líneas telefónicas y Participación de mercado”, Ecuador, 2015.

[8] Agencia de regulación y control de las telecomunicaciones, “Líneas activas por servicio”, Ecuador, 2015.

[9] Ecuador. Agencia de Regulación y Control de las telecomunicaciones. Boletín, marzo de 2015, num. 4.

[10] P. G. Páez, “EL NEGOCIO DEL FRAUDE EN LA INDUSTRIA DE LAS TELECOMUNICACIONES”, Pirámide digital.

[11] M. J. Meza, “Antecedentes” en Fraude en Telecomunicaciones. Quito, Ecuador: SUPERTEL,2008, pp. 2 - 4.

[12] SUPERINTENDENCIA DE TELECOMUNICACIONES, "Compendio histórico de las telecomunicaciones en Ecuador", Publicaciones Institucionales, 2007.

[13] J. Morales. (2011, Diciembre). Bypass Telefónico en Samanes. Ecuador. EXTRA [Online]. Disponible en: http://www.extra.ec/ediciones/2011/12/15/cronica/Bypass-telefonico-en-samanes-v/

[14] R. Pérez, comunicación personal, 12 de enero de 2016.

[15] J. Morales. (2011, Diciembre). Técnicos especialistas de la SUPERTEL desactivaron los equipos de la central clandestina [Fotografía]. Recuperada de:http://www.extra.ec/ediciones/2011/12/15/cronica/Bypass-telefonico-en-samanes-v/

[16] C. M. Criollo, “El Bypass en redes telefónicas celulares. Técnicas de detección de números celulares implicados y de infraestructuras ilegales”, Tesis de pregrado, Fac. Ing. eléctrica y electrónica, Escuela Politécnica Nacional, Quito, Ecuador, 2008.

[17] EKOFON. Tarjeta telefónica saludo [Imagen]. Recuperada de: http://ekofon.com.mx/usuarios-tarjeta-telefonica-saludo.html

[18] (2012, Abril). La Supertel intervino un bypass telefónico en Quito. Ecuador. El Comercio [Online]. Disponible en: http://www.elcomercio.com/actualidad/negocios/supertel-intervino-bypass-telefonico-quito.html

[19] Skype. [Imagen]. Recuperado de: https://secure.Skype.com/es/calling-rates?wt.mc_id=legacy

[20] (2012, Noviembre 19). Ecuador. El empadronamiento redujo el robo, pero aún se activan celulares. El Comercio [Online]. Disponible en: http://www.elcomercio.com/app_public_pro.php/actualidad/seguridad/empadronamiento-redujo-robo-se-activan.html

[21] J. Barona. (2014, Marzo 24). Ecuador. Ecuador le declara la guerra al robo de teléfonos celulares. Agencia Pública de Noticias del Ecuador y Suramérica. [Online]. Disponible en: http://www.andes.info.ec/fr/node/28760

[22] (2015, Junio 17). Ecuador. 238 423 celulares fueron robados en este 2015. El Comercio [Online]. Disponible en: http://www.elcomercio.com/actualidad/robo-celulares-operadoras-delincuencia-comercializacion.html

[23] El Heraldo (2015, Abril).Honduras: Con clonación de IMEI burlan “lista negra” de celulares. El Heraldo [Online]. Disponible: http://www.elheraldo.hn/alfrente/830288-209/honduras-con-clonaci%C

[24] C. Herrera, E. Orquera, L. Estévez (2015, Febrero). Análisis de Protocolos de Señalización para la detección de comportamientos irregulares en líneas de telefonía fija, utilizando sondas de señalización [Online]. 35(1). Disponible: http://www.revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/viewFile/380/pdf

[25] M. J. Meza, “Fraude a las plataformas” en Fraude en Telecomunicaciones. Quito, Ecuador: SUPERTEL, 2008, pp. 23, 24.

[26] makeITsecure. PBX security [Online].Disponible en: http://www.makeitsecure.org/en/pbx-security.html

[27] M. J. Meza, “Fraudes a las plataformas” en Fraude en Telecomunicaciones. Quito, Ecuador: SUPERTEL, 2008, pp. 46, 47.

[28] Voip ms wiki. (2014, Julio 23). False Answer Supervision FAS [Online]. Disponible en: http://wiki.voip.ms/article/False_Answer_Supervision_FAS

[29] Astar. (2012, Febrero 1). Fake False Answer Supervision (FAS) service [Online]. Disponible en: http://www.voip-info.org/wiki/view/Fake+False+Answer+Supervision+(FAS)+service

[30] M. L. Cabello, “Desarrollo de un sistema de medición, monitorización y gestión de servicios OTT”, Anteproyecto, Universidad autónoma de Madrid, Madrid, España.

[31] “OTT Bypass Detection Service Presentation”, Araxxe, v2.2, 2015

[32] Viber, Quiénes somos [Online]. Disponible en: https://www.viber.com/es/about

[33] J. Crook. (2013, Julio 3). Viber Is Testing New Revenue Models, Value-Add Features By Integrating With Traditional Telephony [Online]. Disponibleen:http://techcrunch.com/2013/07/03/viber-is-testing-new-revenue-models-value-add-features-by-integrating-with-traditional-telephony/

[34] Araxxe. DESVÍO DE OTT [Online]. Disponible en:http://www.araxxe.com/desvio-de-ott-40d8da146a3b004923e6e4b32c1071e9.html

[35] M. J. Meza, “Fraudes a las plataformas” en Fraude en Telecomunicaciones. Quito, Ecuador: SUPERTEL, 2008, pp. 13, 14.

[36] M. J. Meza, “Fraudes a las plataformas” en Fraude en Telecomunicaciones. Quito, Ecuador: SUPERTEL, 2008, pp. 8 - 12

[37] M. J. Sánchez, “Utilización del equipo para drive test en la ubicación geográfica de números con actividad irregular reportados por las operadoras de SMA a la SUPERTEL”, Tesis de Pregrado, Fac. Ing. eléctrica y electrónica, Escuela politécnica nacional, Quito, Ecuador, 2013.

[38] “Evolución de los ilícitos en telecomunicaciones en el ecuador”, ARCOTEL, 2015.

[39] C. Ayer. (2015). PBX Fraud Detection. Pipeline. Vol. 12(5). Disponible en:http://media.pipeline.pubspoke.com/files/issue/107/PDF/PipelineNovember2015_A6.pdf

[40] Movistar. [Imagen]. Recuperado de: http://www.movistar.co/documents/44003/314180/anexo_antifraude.pdf

[41] Movistar. ANEXO DE CONDUCTAS NO AUTORIZADAS PARA EL CLIENTE [Online]. Colombia. Disponible en: http://www.movistar.co/documents/44003/314180/anexo_antifraude.pdf

[42] L. Muñoz, comunicación personal, 29 de Diciembre de 2015.

[43] Teleco. Fraude: Sistemas Antifraude [Online]. Disponible en: http://www.teleco.com.br/es/tutoriais/es_tutorialfraude/pagina_4.asp

[44] EKOFON. ¿Qué es la tarjeta telefónica Saludo? [Online]. Disponible en: http://ekofon.com.mx/usuarios-tarjeta-telefonica-saludo.html

[45] J. Schenone. (2012, Noviembre 19). [Imagen]. Recuperado de: http://jose.ryalsche.com/2012/11/instalacion-de-asterisk-en-10-sobre.html

[46] CDR, Call Detail Record, Registro de llamadas [Online]. Disponible en: http://www.telefoniavozip.com/glosario-voip/c/call-detail-record.htm

[47] P. Umanzor. (2012).Asterisk Real time CDR [Imagen]. Recuperado de: http://asterisk-rd.blogspot.com/2012/03/asterisk-realtime-cdr.html

[48] AliExpress. [Fotografía]. Recuperado de: http://es.aliexpress.com/item/Asterisk-Card-PCI-E-4-FXS-FXO-card-410p-a400p-PCI-Express-1X-DIGIUM-400E/1680607157.html?spm=2114.43010208.4.42.Bb4SLF

[49] Avanzada7. [Fotografía]. Recuperado de: http://www.avanzada7.com/es/productos/tarjetas/gsm/sangoma-w400-gsm

[50] Matrix Telecom Solution. Simado GFX11 [Fotografía]. Recuperado de: http://www.matrixtelecom.hu/letolt/manualen/MATRIX%20SIMADO%20GFX11%20SYSTEM%20MANUAL%20EN.pdf

[51] OpenVox. [Fotografía]. Recuperado de: http://www.amazon.com/OpenVox-VS-GW1600-20G-VoxStack-Port-Gateway/dp/B00I87N3RY

ANEXO A: ÍNDICE DE ABREVIATURAS

ARCOTEL	Agencia de Control y Regulación de las Telecomunicaciones
ASR	Answer-seizure ratio
CDR	Call Detail Record
CFCA	Communications Fraud Control Association
CMD	Command Prompt
CNT	Corporación Nacional de Telecomunicaciones
CONECEL	Consorcio Ecuatoriano de Telecomunicaciones
GSM	Global System for Mobile
IMEI	International Mobile System Equipment Identity
ISP	Internet Service Provider
IVR	Interactive voice response
OTT	Over the Top
PBX	Private Branch Xchange
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network

SIM	Subscriber Identity Module
SUPERTEL	Superintendencia de Telecomunicaciones
UIT	Unión Internacional de Telecomunicaciones
VoIP	Voice over IP

ANEXO B: ÍNDICE DE FIGURAS

Figura 1.1: Evolución de la telefonía fija y móvil en el mundo (por cada 100 habitantes) [1]. 1
Figura 1.2: Métodos de Fraudes en telecomunicaciones más comunes en el mundo (2015) 3
Figura 1.3: Pérdidas estimadas en Billones de dólares por método de fraude (2015) [4]. 3
Figura 1.4: Evolución del fraude en telefonía 6
Figura 1.5: Sistema Bypass detectado en un sector de la ciudad de Guayaquil. [15] 8
Figura 1.6: Etapas presentes en el Bypass internacional entrante [16]. 9
Figura 1.7: Tarjetas prepago para llamadas internacionales [17] 10
Figura 1.8: Esquema de Bypass Internacional Entrante 11
Figura 1.9: Elementos de red utilizados en las estaciones Bypass a través de bases celulares. 13
Figura 1.10: Llamada entrante Internacional Bypass por líneas celulares. 14
Figura 1.11: Tarifas deSkype para llamar a Ecuador [19] 15
Figura 1.12: Bypass realizado a través de aplicaciones para smartphones. 16
Figura 1.13: Cajas utilizadas para la liberación de las diferentes marcas de celulares. 19
Figura 1.14: Diagrama del Fraude de Tercer País 19
Figura 1.15: Esquema de una PBX sin alterar. 22
Figura 1.16: Esquema de una PBX hackeada por el método de transferencia de llamada. 22
Figura 1.17: Diagrama de Refilling por Voz sobre IP 23
Figura 1.18: Diagrama de Fraude por Roaming 25
Figura 1.19: Escenario de Falsa Respuesta a llamada 26
Figura 1.20: Aplicación Viber Móvil 28
Figura 1.21: Diagrama de fraude por OTT. 29
Figura 1.22: Diagrama del Fraude de Suscripción. 30
Figura 2.1: Ciclo de vida de la Gestión del Fraude. 37
Figura 2.2: Checklist técnico establecido por movistar Colombia par prevenir fraude en centrales PBX. [40] 42
Figura 2.3: Diagrama del sistema Loop de llamadas automatizado 47
Figura 2.4: Tarjetas pre pagadas para realizar llamadas internacionales [44]. 48
Figura 2.5: Log de llamadas en Asterisk [45]. 49
Figura 2.6: Sistema Loop de llamadas automatizado [14] 50
Figura 2.7: CallDetail Record [47] 51
Figura 2.8: Análisis de CDRs Internacionales [14] 52
Figura 2.9: Análisis de CDRs Internacionales diferenciales [14] 53
Figura 2.10: Tráfico telefónico total (entrante y saliente) [16] 54

Figura 2.11: Sistema de detección de fraude Bypass por Smartphone 57
Figura 2.12: Script para realizar llamadas automáticas.....58
Figura 2.13: Múltiples usuarios Skype listos para realizar llamadas.....58
Figura 2.14: Mensaje de confirmación de llamada en Skype 59
Figura 2.15: Identificación del puerto utilizado para cursar el tráfico Skype 59
Figura 2.16: Análisis en Wireshark del tráfico Skype generado a través del puerto identificado 60
Figura 2.17: Tarjeta telefónica analógica Digium TDM404 [48].....61
Figura 2.18: Topología del diseño de detección para Fraude OTT 63
Figura 2.19: Tarjeta GSM SANGOMA W400. [54] 64
Figura 2.20: Base celular GSM GFX11 de 1 puerto SIM. [55].....65
Figura 2.21: Gateway OpenVox VS-GW1600-20G. [56] 65
Figura 2 22: Pantalla de activación de Viber en el escritorio 66
Figura 2.23: Aplicación Qustodio instalada en Smartphone. 67
Figura 2.24: Cronología de la actividad para un usuario 68
Figura 2.25: Configuración de notificación de Qustodio 68

ANEXO C: ÍNDICE DE TABLAS

Tabla 1: Operadoras de servicio de telefonía fija en el país [6].....4
Tabla 2: Cobro por recepción de llamadas con la red de datos móvil 29
Tabla 3: Métodos de comunicación no autorizados por la operadora OTECEL a sus clientes [41].....45
Tabla 4: Precios de los recursos para sistema de detección de fraude desde smartphone.....71
Tabla 5: Precios de los recursos para sistema de detección de fraude OTT.....72