REPÚBLICA DEL ECUADOR
Escuela Politécnica Nacional
"E SCIENTIA HOMINIS SALUS"

La versión digital de esta tesis está protegida por la Ley de Derechos de Autor del Ecuador.

Los derechos de autor han sido entregados a la "ESCUELA POLITÉCNICA NACIONAL" bajo el libre consentimiento del (los) autor(es).

Al consultar esta tesis deberá acatar con las disposiciones de la Ley y las siguientes condiciones de uso:

- Cualquier uso que haga de estos documentos o imágenes deben ser sólo para efectos de investigación o estudio académico, y usted no puede ponerlos a disposición de otra persona.
- Usted deberá reconocer el derecho del autor a ser identificado y citado como el autor de esta tesis.
- No se podrá obtener ningún beneficio comercial y las obras derivadas tienen que estar bajo los mismos términos de licencia que el trabajo original.

El Libre Acceso a la información, promueve el reconocimiento de la originalidad de las ideas de los demás, respetando las normas de presentación y de citación de autores con el fin de no incurrir en actos ilegítimos de copiar y hacer pasar como propias las creaciones de terceras personas.

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS DE PROTOCOLOS DE SEÑALIZACIÓN PARA LA DETECCIÓN DE COMPORTAMIENTOS IRREGULARES EN LAS LÍNEAS DE TELEFONÍA FIJA, EN EL SOFTSWITCH DE QUITO PERTENECIENTE A LA CNT EP, UTILIZANDO SONDAS DE SEÑALIZACIÓN

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

ORQUERA SERRANO EDWIN FERNANDO

(tano_1821@hotmail.com)

DIRECTOR: ING. LUIS GEOVANNI ESTÉVEZ ORQUERA

(luis.estevez@cnt.gob.ec)

CODIRECTOR: ING. CARLOS ALFONSO HERRERA MUÑOZ

(carlos.herrera@epn.edu.ec)

Quito, diciembre 2014

DECLARACIÓN

Yo, Edwin Fernando Orquera Serrano, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Edwin Fernando Orquera Serrano

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Edwin Fernando Orquera Serrano, bajo mi supervisión.

_____	_____
Ing. Luis Geovanni Estévez Orquera	**Ing. Carlos Alfonso Herrera Muñoz**
DIRECTOR DEL PROYECTO	**CODIRECTOR DEL PROYECTO**

AGRADECIMIENTO

Agradezco a Dios por permitirme culminar mi carrera, por las duras pruebas que puso en mi camino y que me ayudaron a forjar mi carácter, gracias por jamás soltar mi mano.

A mi madre Tere, gracias por todo el amor constante e incondicionalque me has brindado, por tantas noches de desvelo a mi lado, pordedicar tu vida entera para mí, por ser mi ángel guardián siempre. Te admiro por ser la mejor madre: tierna, dulce y justa, sin ti no hubiera podido concluir esta meta, te amo mucho.

A mi padre Edwin. Eres un gran padre y amigo; gracias por apoyarme en cada una de mis decisiones de forma incondicional;gracias por todos los consejos que me has brindado. Gracias por todos los esfuerzos que has tenido que realizar en cada etapa de mi vida para verme salir adelante. Te amo mucho.

A mi amada esposa Carolina, gracias por darme una hermosa familia, por brindarme tu amor incondicionalmente; por recorrer a mi lado tantos años hermosos y difíciles, por decidir enfrentar muchos obstáculos de mi mano. Eres una gran mujer y madre, te amo.

A mis queridos amigos, gracias por todos los momentos compartidos dentro y fuera de la universidad durante todos estos años. Su amistad verdadera fue uno de los pilares fundamentales para concluir este proyecto en mi vida.

A la Escuela Politécnica Nacional y mis maestros por todos los conocimientos otorgados. De forma muy especial al Ing. Carlos Herrera por guiar de forma muy acertada este proyecto de titulación. Agradezco por su transparencia y desprendimiento con el cual aceptó colaborarme.

Finalmente agradezco a la Corporación Nacional de Telecomunicaciones; a todos los ingenieros que conforman el Departamento de Prevención de Fraude que supieron brindarme la ayuda necesaria. De manera especial al Ing. Luis Estévez por todas las facilidades prestadas al dirigir el presente trabajo con tanto interés, entusiasmo y sencillez, demostrando ser un gran ser humano.

Fernando Orquera

DEDICATORIA

A mis hijos, Milena y Matías, por ser mi más grande motivación para salir adelante durante todos estos años. Sus risas, sus travesuras, sus gestos de amor y dulzura hacia mí fueron mi mayor soporte en los momentos difíciles. De igual manera a mi esposa Carolina por estar a mi lado de forma incondicional durante todos estos años. Los amo con mi alma entera!!.

A mis padres por todos los esfuerzos que han tenido que realizar para ayudarme a alcanzar mis metas, por todo el amor que me han brindado durante mi vida. Mi justa y eterna gratitud hacia ustedes por apoyar cada paso y decisión tomada, la vida se encargará de retribuirles todas las bendiciones que han derramado sobre mí; ustedes son y serán mi mayor ejemplo a seguir.

Fernando Orquera

ÍNDICE DE CONTENIDOS

DECLARACIÓN. i

CERTIFICACIÓN. ii

AGRADECIMIENTOS..... iii

DEDICATORIA..... iv

ÍNDICE DE CONTENIDOS. v

ÍNDICE DE FIGURAS. xi

ÍNDICE DE TABLAS. xv

PRESENTACIÓN. xvii

RESUMEN. xviii

CAPÍTULO 1

ESTUDIO DE LOS PROTOCOLOS DE SEÑALIZACIÓN

1.1 TELEFONÍA TRADICIONAL. 1

1.1.1 TELEFONÍA DIGITAL. 1

1.1.1.1 Red digital de servicios integrados*(RDSI – ISDN).* 1

1.1.1.1.1 Canales de transmisión. 2

1.2 TELEFONÍA IP..... 4

1.2.1 VOIP (VOZ SOBRE IP) 4

1.2.1.1 Características de VoIP..... 4

1.2.1.2 Arquitectura de VoIP. 4

1.2.2 TELEFONÍA SOBRE IP 5

1.2.2.1 Proceso de llamada en Telefonía IP. 6

1.2.2.2 Tipos de llamadas en Telefonía IP. 8

1.3 SEÑALIZACIÓN EN TELEFONÍA 8

1.3.1 TIPOS DE SEÑALIZACIÓN..... 9

1.3.1.1 Señalización de abonado 9
1.3.1.2 Señalización entre centrales. 9
1.3.1.2.1 Señalización asociada al canal. 10
1.3.1.2.2 Señalización por canal común. 10
1.4 PROTOCOLOS DE SEÑALIZACIÓN 11
1.4.1 PROTOCOLO SS7 11
1.4.1.1 Generalidades. 11
1.4.1.2 Componentes de una red de señalización SS7. 12
1.4.1.2.1 Puntos de señalización 12
1.4.1.2.2 Enlaces de señalización: 12
1.4.1.3 Arquitectura de protocolos SS7 13
1.4.2 PROTOCOLO MEGACO/ H.248. 14
1.4.2.1 Generalidades. 14
1.4.2.2 Componentes que intervienen en sistema MEGACO. 15
1.4.2.3 Estructura del mensaje H.248/MEGACO 15
1.4.2.3.1 Transacciones en el mensaje 16
1.4.2.3.2 Instrucciones MEGACO 17
1.4.3 PROTOCOLO SIGTRAN. 18
1.4.3.1 Generalidades. 18
1.4.3.2 Componentes de la arquitectura de SIGTRAN. 18
1.4.3.2.1 Protocolo SCTP 19
1.4.3.2.2 Protocolo M2PA 22
1.4.3.2.3 Protocolo M2UA 23
1.4.3.2.4 Protocolo M3UA. 28
1.4.3.2.5 Protocolo IUA. 32
1.4.3.2.6 Protocolo SUA. 35
1.4.4 PROTOCOLO SIP 40

1.4.4.1 Generalidades. 40
1.4.4.2 Componentes de una red SIP 41
1.4.4.3 Mensajes SIP 44
1.4.4.3.1 Estructura de los mensajes SIP. 44

CAPÍTULO 2

MÉTODOS DE CONTROL DE FRAUDE EN EL TRÁFICO TELEFÓNICO

2.1 INTRODUCCIÓN. 52
2.2 CONCEPTO DE FRAUDE 52
2.2.1 FRAUDE. 52
2.2.2 FRAUDE EN TELECOMUNICACIONES 52
2.3 TRIÁNGULO DEL FRAUDE. 53
2.4 CONTROL DE FRAUDE 54
2.5 DEPARTAMENTO DE PREVENCIÓN DE FRAUDE. 55
2.6 MARCO REGULATORIO PARA FRAUDES EN TELECOMUNICACIONES. 56
2.7 TIPOS DE FRAUDES EN TELEFONÍA. 56
2.7.1 FRAUDE POR SUSCRIPTOR. 56
2.7.1.1 Detección y control. 57
2.7.2 FRAUDE CLIP-ON. 57
2.7.2.1 Detección y control. 58
2.7.3 FRAUDE DE TERCER PAÍS. 58
2.7.3.1 Detección y control. 59
2.7.4 FRAUDE DE PBX. 59
2.7.4.1 Detección y control. 60
2.7.5 BY PASS 60
2.7.5.1 Ruta legal de una llamada internacional. 62
2.7.5.2 Ruta ilegal de una llamada internacional. 63

2.7.5.3 Detección y control. 64

2.8 MÉTODOS DE CONTROL DE FRAUDE EN TELECOMUNICACIONES. 64

2.8.1 LLAMADAS DE PRUEBA DE TRÁFICO TELEFÓNICO INTERNACIONAL. 65

2.8.1.1 Pruebas de lazo telefónico internacional (loop). 65

2.8.1.2 Bombardeo de llamadas. 66

2.8.2 PERFILAMIENTO DE TRÁFICO TELEFÓNICO. 67

2.8.2.1 Análisis de CDRs. 68

CAPÍTULO 3

ANÁLISIS DE LOS PROTOCOLOS DE SEÑALIZACIÓN DENTRO DE LA RED DE SERVICIOS TELEFÓNICOS DE CNT MEDIANTE EL USO DE SONDAS DE SEÑALIZACIÓN.

3.1 DESCRIPCIÓN DEL EQUIPO. 71

3.1.1 CARACTERÍSTICAS GENERALES. 71

3.1.2 INTERFACES DE MEDICIÓN SOPORTADAS. 72

3.1.3 COMPONENTES FÍSICAS DE PANTERA 100. 72

3.1.4 PROTOCOLOS SOPORTADOS. 73

3.2 CONFIGURACIÓN PARA PRUEBAS DE MONITOREO. 73

3.3 OBTENCIÓN DE LOS RESULTADOS. 78

3.4 ANÁLISIS TEÓRICO DE LOS PROTOCOLOS DE SEÑALIZACIÓN PARA LA OBTENCIÓN DE CDRs. 79

3.4.1 PROTOCOLOS SIGTRAN 79

3.4.2 PROTOCOLO SIP. 85

3.5 BASE DE DATOS PARA LOS CDRs. 89

3.5.1 GENERACIÓN DE LA BASE DE DATOS. 90

3.5.1.1 Creación de una nueva base de datos. 90

3.5.1.2 Importación de datos externos hacia la base de datos. 90

3.5.1.2.1 Importación simultánea de varios archivos de texto. 94

CAPÍTULO 4

DETECCIÓN DE POSIBLES USOS INDEBIDOS DEL SERVICIO DE TELEFONÍA FIJA EN CNT MEDIANTE EL ANÁLISIS DE CDRS.

4.1 INTRODUCCIÓN 96

4.2 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE CLIP ON. 97

4.2.1 PATRÓN DE COMPORTAMIENTO. 97

4.2.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS. 98

4.2.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE CLIP ON. 100

4.2.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE CLIP ON. 102

4.3 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE PBX. 105

4.3.1 PATRÓN DE COMPORTAMIENTO. 105

4.3.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS. 106

4.3.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE PBX. 108

4.3.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE DE PBX. 113

4.4 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE BYPASS. .. 115

4.4.1 PATRÓN DE COMPORTAMIENTO. 115

4.4.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS. 116

4.4.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE BY PASS ENTRANTE. 117

4.4.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE BYPASS ENTRANTE. 119

4.5 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE DE TERCER PAÍS. 120

4.5.1 PATRÓN DE COMPORTAMIENTO. 120

4.5.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS. 121

4.5.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE DE TERCER PAÍS. 123

4.5.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE DE TERCER PAÍS. 125

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES.

5.1 CONCLUSIONES. 127

5.2 RECOMENDACIONES. 130

BIBLIOGRAFÍA 131

GLOSARIO DE TÉRMINOS.....138

ANEXOS.....140

ÍNDICE DE FIGURAS

CAPÍTULO 1

ESTUDIO DE LOS PROTOCOLOS DE SEÑALIZACIÓN.

Figura 1.1 Arquitectura VoIP 5
Figura 1.2 Proceso de llamada IP 6
Figura 1.3 TCP/IP en telefonía IP 7
Figura 1.4 Llamadas de PC a PC 8
Figura 1.5 Llamada de teléfono a teléfono 8
Figura 1.6 Llamada de PC a teléfono 8
Figura 1.7 Funciones de la señalización 9
Figura 1.8 Esquema de señalización E1 10
Figura 1.9 Puntos de señalización. 12
Figura 1.10 Stack de protocolos SS7 13
Figura 1.11 Componentes de MEGACO 15
Figura 1.12 Estructura mensaje H.248/MEGACO 16
Figura 1.13 Arquitectura de SIGTRAN 19
Figura 1.14 Estructura paquete SCTP 20
Figura 1.15 Protocolos en la capa de adaptación. 21
Figura 1.16 Comunicación mediante M2PA 22
Figura 1.17 Cabecera M2PA 23
Figura 1.18 Proceso de comunicación con M2UA 24
Figura 1.19 Cabecera Común M2UA 24
Figura 1.20 Formato de los parámetros de longitud variable M2UA 27
Figura 1.21 Transporte con M3UA hacia una capa MTP3 remota 28
Figura 1.22 Estructura de la cabecera M3UA 29
Figura 1.23 Estructura parámetros de longitud variable M3UA 31
Figura 1.24 Estructura de la cabecera IUA 32
Figura 1.25 Estructura parámetros de longitud variable IUA 34
Figura 1.26 Transporte de señalización mediante SUA. 36
Figura 1.27 Cabecera común de mensajes SUA 36
Figura 1.28 Estructura parámetros de longitud variable SUA 39
Figura 1.29 SIP dentro de la arquitectura TCP/IP 41

Figura 1.30 Comunicación entre UAC y UAS 41
Figura 1.31 Comunicación SIP mediante servidor proxy. 42
Figura 1.32 Comunicación SIP mediante servidor de redirección. [28] 43
Figura 1.33 Comunicación mediante un servidor de registro 43
Figura 1.34 Formato mensajes SIP 44
Figura 1.35 Estructura de línea de solicitud de mensajes SIP 44
Figura 1.36 Estructura de línea de estado de mensajes SIP 46
Figura 1.37 Ejemplo de un mensaje de solicitud SIP 50
Figura 1.38 Ejemplo de un mensaje de respuesta SIP 51

CAPÍTULO 2

MÉTODOS DE CONTROL DE FRAUDE EN EL TRÁFICO TELEFÓNICO

Figura 2.1 Triángulo del Fraude 54
Figura 2.2 Proceso de control de fraude 55
Figura 2.3 Fraude por suscripción 57
Figura 2.4 Fraude de Tercer País 58
Figura 2.5 Fraude de PBX 60
Figura 2.6 Componentes Sistema By – Pass 61
Figura 2.7 Equipos de un Sistema By Pass requisado por la SUPERTEL 62
Figura 2.8 Ruta legal de una llamada internacional 62
Figura 2.9 Ruta bypass de una llamada internacional 63
Figura 2.10 Prueba de lazo telefónico internacional. 66
Figura 2.11 Bombardeo de llamadas 67
Figura 2.12 Perfilamiento de tráfico telefónico 68
Figura 2.13 Campos de CDR. 69

CAPÍTULO 3

ANÁLISIS DE LOS PROTOCOLOS DE SEÑALIZACIÓN DENTRO DE LA RED DE SERVICIOS TELEFÓNICOS DE CNT MEDIANTE EL USO DE SONDAS DE SEÑALIZACIÓN.

Figura 3.1 Componentes Físicas de Pantera 100. 72
Figura 3.2 Ventana de Interfaces Físicas Pantera 100 74
Figura 3.3 Configuración de las interfaces físicas de Pantera 100 75

Figura 3.4 Opciones de grabado de archivos 76
Figura 3.5 Opciones de grabados de archivos en SDF 77
Figura 3.6 Configuración de filtrado de resultados. 78
Figura 3.7 Ejecución de la prueba de monitoreo 78
Figura 3.8 Ejemplo de un archivo de texto plano 79
Figura 3.9 Capas de Arquitectura SIGTRAN. 80
Figura 3.10 Datos de llamada telefónica en cabecera común M2UA 81
Figura 3.11 Datos de llamada telefónica en parámetro de longitud variable M2UA 81
Figura 3.12 Datos de llamada telefónica en la trama SCTP. 82
Figura 3.13 Datos de llamada telefónica en datagrama IP 83
Figura 3.14 Establecimiento de una llamada telefónica mediante SIGTRAN. 84
Figura 3.15 Datos de una llamada telefónica en Mensaje de solicitud SIP. 86
Figura 3.16 Datos de una llamada telefónica en Mensaje de respuesta SIP 87
Figura 3.17 Establecimiento de una llamada telefónica mediante SIP. 88
Figura 3.18 Elementos de una tabla 89
Figura 3.19 Creación nueva base de datos 90
Figura 3.20 Importación de datos externos. 91
Figura 3.21 Configuración de importación de archivos externos 91
Figura 3.22 Configuración de especificación para importar datos. 92
Figura 3.23 Configuración de los campos 93
Figura 3.24 Proceso de guardado de la especificación. 93
Figura 3.25 Asignación de nombre de tabla creada. 93
Figura 3.26 Tabla obtenida mediante la importación de archivos de texto. 94
Figura 3.27 Script para importación simultánea de archivos de texto 94
Figura 3.28 Tabla obtenida mediante la importación simultánea de varios de archivos de texto. 95

CAPÍTULO 4

DETECCIÓN DE POSIBLES USOS INDEBIDOS DEL SERVICIO DE TELEFONÍA FIJA EN CNT MEDIANTE EL ANÁLISIS DE CDRS.

Figura 4.1 Diagrama General de la red de telefonía de CNT. 97
Figura 4.2 Comportamiento Fraude Clip On 98

Figura 4.3 Diagrama de flujo para fraude Clip On 101
Figura 4.4 Comportamiento Fraude PBX 106
Figura 4.5 Diagrama de flujo para fraude PBX. 112
Figura 4.6 Comportamiento de líneas telefónicas usadas en fraude By Pass Entrante 115
Figura 4.7 Diagrama de flujo para fraude By Pass. 118
Figura 4.8 Comportamiento Fraude Tercer País 121
Figura 4.9 Diagrama de flujo para fraude de Tercer País. 124

ÍNDICE DE TABLAS.

CAPÍTULO 1

ESTUDIO DE LOS PROTOCOLOS DE SEÑALIZACIÓN.

Tabla 1.1 Tipos de canales de transmisión 2
Tabla 1.2 Estructura de los tipos de acceso..... 3
Tabla 1.3 Instrucciones MeGaCo. 17
Tabla 1.4 Tipos de fragmentos. 21
Tabla 1.5 Clases de mensajes M2UA 25
Tabla 1.6 Tipo de mensajes M2UA 25
Tabla 1.7 Lista de etiquetas de parámetros M2UA 27
Tabla 1.8 Clases de mensaje M3UA 29
Tabla 1.9 Tipos de mensajes M3UA 29
Tabla 1.10 Etiquetas de parámetros M3UA 31
Tabla 1.11 Clases de mensajes IUA 32
Tabla 1.12 Tipos de mensajes IUA 33
Tabla 1.13 Etiquetas de los parámetros IUA..... 35
Tabla 1.14 Clases de mensajes SUA. 37
Tabla 1.15 Tipos de mensajes SUA 37
Tabla 1.16 Métodos de un mensaje de solicitud SIP..... 45
Tabla 1.17 Códigos de estado de un mensaje de respuesta SIP 46
Tabla 1.18 Cabeceras del mensaje SIP 48

CAPÍTULO 2

MÉTODOS DE CONTROL DE FRAUDE EN EL TRÁFICO TELEFÓNICO

Tabla 2.1 Proceso legal de una llamada internacional. 63
Tabla 2.2 Proceso ilegal de una llamada internacional. 64
Tabla 2.3 Campos de CDRs evaluados en cada fraude 70

CAPÍTULO 3

ANÁLISIS DE LOS PROTOCOLOS DE SEÑALIZACIÓN DENTRO DE LA RED DE SERVICIOS TELEFÓNICOS DE CNT MEDIANTE EL USO DE SONDAS DE SEÑALIZACIÓN.

Tabla 3.1 Características Generales PANTERA 100. 72
Tabla 3.2 Protocolos soportados por PANTERA 100. 73
Tabla 3.3 Tiempos de duración de una llamada mediante SIGTRAN 84
Tabla 3.4 Tiempos de duración de una llamada mediante SIP 89

CAPÍTULO 4

DETECCIÓN DE POSIBLES USOS INDEBIDOS DEL SERVICIO DE TELEFONÍA FIJA EN CNT MEDIANTE EL ANÁLISIS DE CDRS.

Tabla 4.1 Umbrales - Restricciones de campos para Fraude Clip On. 99
Tabla 4.2 Números telefónicos resultantes de la consulta. 102
Tabla 4.3 Líneas telefónicas a ser examinadas con detalle. 103
Tabla 4.4 Líneas telefónicas a ser contactadas. 104
Tabla 4.5 Líneas telefónicas a ser inspeccionadas. 105
Tabla 4.6 Líneas telefónicas con fraude Clip On. 105
Tabla 4.7 Umbrales - Restricciones de campos para Fraude PBX. 107
Tabla 4.8 Destinos atípicos para fraude PBX. 109
Tabla 4.9 Números telefónicos resultantes de la consulta para fraude PBX. 113
Tabla 4.10 Líneas con PBX a ser contactadas. 114
Tabla 4.11 Umbrales - Restricciones de campos para Fraude By Pass Entrante. 116
Tabla 4.12 Líneas telefónicas para posterior estudio. 119
Tabla 4.13 Umbrales - Restricciones de campos para Fraude de Tercer País. . 122
Tabla 4.14 Líneas Telefónicas a ser examinadas. 125

PRESENTACIÓN

En el sector de las telecomunicaciones, es necesario tratar y gestionar al fraude con la debida importancia, puesto que este hecho produce pérdidas de alrededor del 4.8% del total de ingresos económicos obtenidos por las empresas que brindan estos servicios.Dichas empresas continuamente buscan implementar a sus procesos de gestión diferentes métodos para detectar conductas inusuales por parte de los suscriptores que puedan reflejar potenciales usos indebidos de los servicios o casos de fraude dentro de las telecomunicaciones y que posteriormente se traducen en pérdidas económicas para las empresas.

A consecuencia de lo expuesto surge el presente Proyecto con el fin de realizar un control de fraude en telefonía fija a bajo nivel mediante el análisis y establecimiento de valores umbrales de varios campos de los registros de llamadas conocidos como CDRs, los cuales son obtenidos al sondear protocolos de señalización, específicamente para el caso, SIP y SIGTRAN.

En este trabajo se estudia conceptos fundamentales sobre la telefonía y su evolución en el transcurso del tiempo hasta llegar a la telefonía sobre IP; además se explica la señalización telefónica con sus respectivos tipos y protocolos utilizados. Finalmente se menciona ideas generales sobre el fraude en telefonía y los diferentes tipos existentes en este campo.

RESUMEN

El avance tecnológico existente ha sido durante los últimos años el pilar fundamental para lograr dar servicios de telecomunicaciones de calidad; en contraste, en el área correspondiente a la telefonía, este avance tecnológico juega un papel antagónico ya que permite desarrollar en mayor número y con mayor eficiencia, sistemas de fraude que ocasionan cuantiosas pérdidas a las empresas que prestan dichos servicios.

El objetivo del presente trabajo se basa en implementar un control de fraudes para telefonía fija mediante el análisis de protocolos de señalización y de esta forma evitar pérdidas económicas en la Corporación Nacional de Telecomunicaciones, empresa en la cual se desarrolló el mencionado control. Para el propósito, el presente Proyecto está dividido en cinco capítulos resumidos de la siguiente manera:

En el capítulo I se realiza una descripción de cada uno de los protocolos de señalización existentes en telefonía haciendo énfasis en los protocolos que se analizan en el trabajo de campo como son: SIP y SIGTRAN; además se detallan los diferentes métodos de señalización así como de los aspectos básicos de la telefonía fija tradicional y de la basada en VoIP.

En el capítulo II se detalla diferentes métodos para controlar el tráfico telefónico y de esta manera evitar posibles usos indebidos del servicio de telefonía que puedan finalmente ser potenciales fraudes. Además se describe algunos tipos de fraude relacionados con el presente Proyecto así como también se realiza una descripción general del fraude en las Telecomunicaciones.

En el capítulo III se analizanlos protocolos de señalización, en base a la utilización de un equipo analizador de protocolos; el cual sondea señalización y extrae datos específicos de los registros de llamadas que son exportados hacia una base de datos con la cual se puede interactuar mediante la programación de cadenas de consultas conocidas como querys y de esta forma se extrae información específica para la detección de actividades fraudulentas mediante el establecimiento de valores umbrales.

En el capítulo IV se realiza el análisis de los registros de llamadas obtenidos, los cuales contienen diferentes campos de información como son: origen, destino, fecha de la llamada, hora de inicio de la llamada, hora de finalización de llamada, duración, entre otros. En función de detectar posibles fraudes, se establecerán valores umbrales para varios de estos campos como son: duración, tipo y hora de llamada. Si al analizar los CDRs se observan valores superiores a los umbrales, se activa una alarma, que debe ser tomada en cuenta para confirmar si existe una actividad fraudulenta. Cuando surge una alarma se realizará un análisis diferencial, en el cual se monitorean patrones de comportamiento de la línea telefónica comparando sus más recientes actividades con la historia de uso de la misma; un cambio en el patrón de comportamiento permitirá detectar escenarios fraudulentos.

En este capítulo V se detallan las conclusiones finales que se derivan del desarrollo del Proyecto; así como también las recomendaciones en cada una de las etapas del mismo.

CAPÍTULO 1.

ESTUDIO DE LOS PROTOCOLOS DE SEÑALIZACIÓN.

1.1 TELEFONÍA TRADICIONAL.

La red telefónica convencional en sus inicios tuvo el propósito de transmitir únicamente información de origen analógico (voz humana). Se basó en una tecnología por conmutación de circuitos que no es otra cosa que mantener un canal reservado entre los dos extremos de la comunicación telefónica mientras dure la conversación teniendo para ello siempre un enlace físico entre los dos.
Con el transcurso del tiempo, los sistemas telefónicos analógicos experimentaron algunos problemas como son: degradaciones en la señal de voz y sobretodo el impedimento de realizar múltiples llamadas frente a la gran demanda telefónica existente por lo cual se origina la telefonía digital que vino a solventar las necesidades que existían en ese entonces.

1.1.1 TELEFONÍA DIGITAL.

El primer paso para poder desarrollar la telefonía digital fue precisamente digitalizar la información a ser transmitida, es decir la voz; para ello es necesario seguir un proceso de cuatro pasos que son:

a) Muestreo: Se toma una muestra cada 125µs.
b) Cuantificación: Se le asigna un valor cuántico a cada muestra.
c) Codificación:Se asigna un código binario a cada valor cuantificado.
d) Compresión: Se reduce la cantidad de bits de la información antes de transmitirla.

1.1.1.1 Red digital de servicios integrados(RDSI – ISDN).[1]

El hecho de transmitir voz digital fue determinante para lograr incorporar voz y datos en una misma línea; y con ello tener una gama de servicios a disposición del usuario llamados de valor agregado. Las principales características de la RDSI son:

- Conectividad digital extremo a extremo.

- Incorporación de elementos de conmutación de paquetes.
- Conexiones por conmutación de circuitos a 64 kbps.
- Diferentes vías para señalización y transferencia de información.

1.1.1.1.1 Canales de transmisión. [1][2]

Existen tres diferentes tipos de canales para transmitir datos:

Canales B: Transmiten información a 64 kbps (datos de voz o datos informáticos)

Canales D: Trabajan a 16 kbps o 64 kbps. Se los utiliza para dos propósitos. Primero para la señalización de llamadas de circuitos conmutados. También pueden transmitir datos cuando no se los utiliza para control.

Canales H: Combinaciones de múltiples canales tipo B para transmitir información de audio de alta calidad o video a altas velocidades. Existen varios tipos:

- Canales H0, trabajan a 384 kpbs (6 canales B)
- Canales H10, trabajan a 1472 kbps (23 canales B)
- Canales H11, trabajan a 1536 kbps (24 canales B)
- Canales H12, trabajan a 1920 kbps (30 canales B)

En la tabla 1.1 se indica los tipos de canales de transmisión con sus respectivas velocidades.

TIPO	FUNCIÓN	VELOCIDAD
B	Servicios Básicos	64 Kbps.
D	Señalización	16 Kbps. (BRI) 64 Kbps. (PRI)
H_o	6 Canales B	384 Kbps. (PRI)
H_1	Todos los Canales Ho H_{11} (24 B) H_{12} (30B)	 1.536 Kbps. (PRI) 1.920 Kbps. (PRI)
H_2	RDSI de Banda Ancha H_{21} H_{22}	(propuesta actual) 32.768 Kbps. 43-45 Mbps.
H_4	RDSI de Banda Ancha	132-138,240 Mbps.

Tabla 1.1 Tipos de canales de transmisión [2]

Al usuario final se ofrecen estructuras de transmisión conformadas por agrupaciones de los canales tratados; para este fin se definen dos accesos fundamentales: acceso básico y acceso primario.

Acceso Básico en RDSI*(BRI).*[1]

Consta de dos canales B full-dúplex de 64 kbps y un canal D full-dúplex de 16 kbps. El acceso básico consiste en dos canales B full-dúplex de 64 kbps y un canal D full-dúplex de 16 kbps. La UIT-T define este tipo de acceso en su recomendación I.420.

Acceso Primario en RDSI*(PRI).*[1]

Utilizado para usuarios que necesitan capacidades mayores. Soporta hasta 30 canales D y tres canales H. Estados Unidos, Japón y Canadá usan un canal T1 de 1.544 Mbps (23 canales B más un canal D de 64 kbps), mientras que en Europa la velocidad estándar de un canal E1 es 2.048 Mbps (30 canales B más un canal D de 64 kbps). En la tabla 1.2 se resume los diferentes tipos de acceso con sus respectivas estructuras de transmisión:

ACCESO	ESTRUCTURA		VELOCIDAD TOTAL	VELOCIDAD DISPONIBLE
Básico (BRI)	2B + D(16)		192 kbps	144 kbps
Primario (PRI)	T1	23B + D(64)	1544 kbps	1536 kbps
	E1	30B + D(64)	2048 kbps	1984 kbps

Tabla 1.2 Estructura de los tipos de acceso

En Ecuador se ha adoptado como estándar de transmisión el canal E1. La trama E1 consta en 32 divisionesde 64kbps cada una, dentro del cual existen 30 líneas de teléfono normales más 2 canales de señalización que usan las centrales para comunicarse entre ellas mediante un protocolo definido como SS7, el cual se lo presentará posteriormente.

1.2 TELEFONÍA IP

1.2.1 VOIP (VOZ SOBRE IP) [3]

La voz sobre IP es una tecnología que permite transportar a través de redes IP, paquetes de datos comprimidos, resultado de convertir lospaquetes de voz estándar haciendo uso del protocolo IP. Es decir que este tipo de tecnología se basa en conmutación de paquetes.

1.2.1.1 Características de VoIP.

Este tipo de tecnología como tal presenta muchas ventajas como son:

- Evita los cargos altos de telefonía que se presentan generalmente en comunicaciones a larga distancia.
- Independenciafrente al hardware utilizado.
- Simplificación en la infraestructura frente a la necesaria en una central tradicional. Esto se debe a que en esta nueva tecnología solo se utiliza un software instalable en un servidor con los mismos usos.
- Optimización en el rendimiento ya que se puede controlar el tráfico de la red.
- Transparencia al tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
- Proporciona un enlace a la red de telefonía tradicional.

1.2.1.2 Arquitectura de VoIP.

Los diferentes elementos que conforman una arquitectura VoIP son:

Gateway: El Gateway es un dispositivo fundamental en la arquitectura de VoIP encargado de convertir la información de voz entre la red telefónica pública conmutada y la red VoIP.

Servidor: Este elemento se encarga del manejo y la gestión de los recursos de red. Las principales funciones otorgadas a este elemento son: registro, control de llamadas, enrutamiento entre otras.

Terminales de VoIP: Son los dispositivos finales que actúan como clientes ya sean estos representados en software o hardware.

En la figura 1.1 se ilustra una arquitectura de un sistema de voz sobre IP.

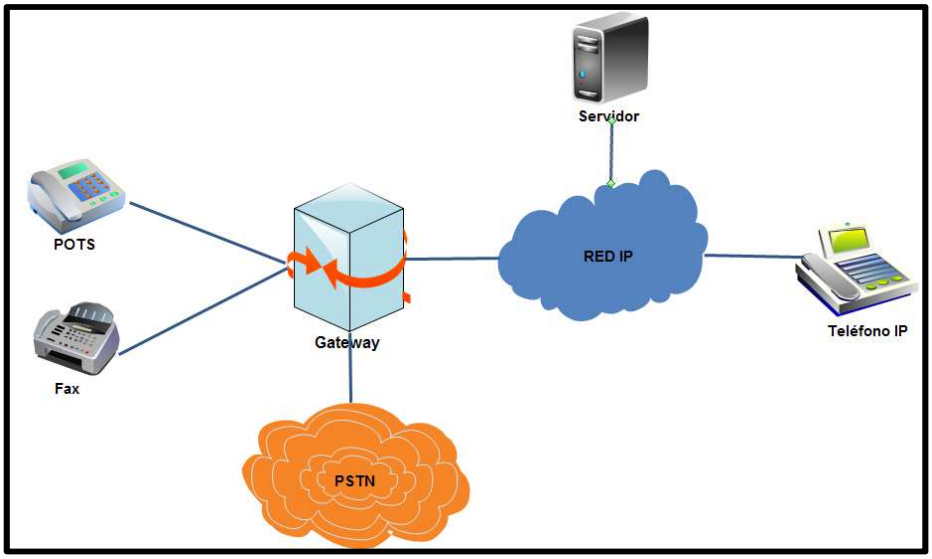

Figura 1.1 Arquitectura VoIP

Se debe tener clara la diferencia esencial entre VoIP que es la tecnología, con sus respectivas normas y protocolos, que permite comunicar voz sobre el protocolo IP y telefonía sobre IP que es el servicio telefónico disponible al público, realizado con tecnología de VoIP.

1.2.2 TELEFONÍA SOBRE IP [3] [4]

La telefonía IP se basa en comunicaciones telefónicas realizadas a través de redes TCP/IP. La información que se transmite a través de la red se divide en paquetes de datos los cuales tienen un encabezado que abarca el origen y el destino, un número de secuencia, un bloque de datos y un código de comprobación de errores. Los enrutadores envían estos paquetes a través de la red hasta que llegan a su destino en donde se utilizará el número de secuencia para volver a unirlos en su orden original. Los paquetes de datos comparten un circuito con otras transmisiones a diferencia de la telefonía tradicional que brinda un circuito a cada llamada telefónica.

La importancia de la Telefonía IP radica en la reducción los costos de las llamadas (hasta en un 74%), cuyo precio no depende del tiempo de conexión; por

lo cual la reducción en costos puede ser considerable, especialmente para las compañías con sucursales en distintas ciudades o países.

1.2.2.1 Proceso de llamada en Telefonía IP.[3] [5]

En la figura 1.2 se puede observar el proceso desarrollado en una llamada telefónica IP.

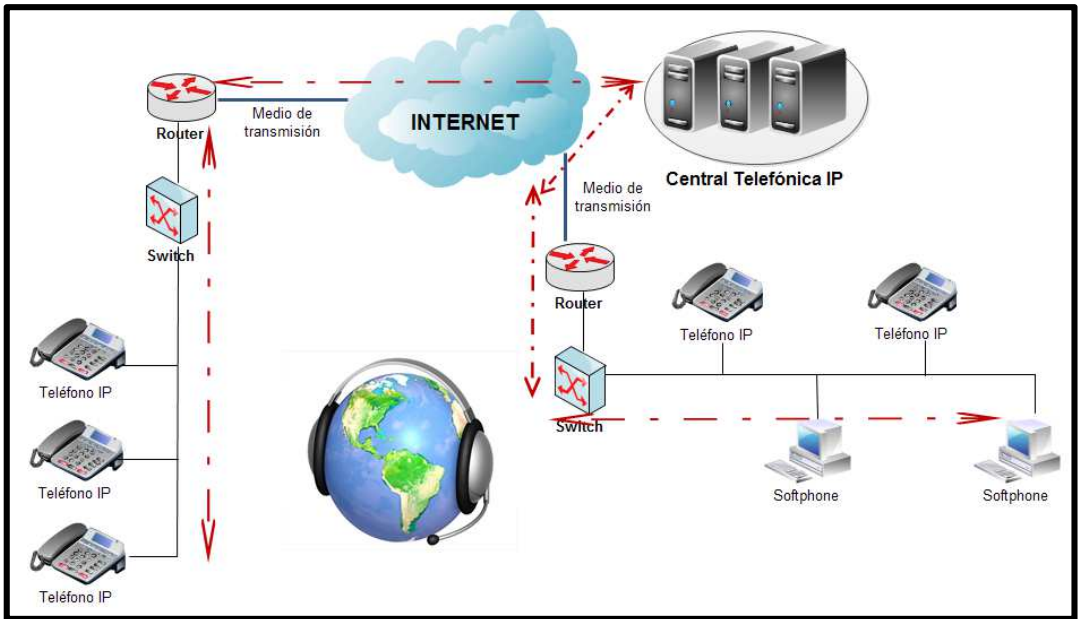

Figura 1.2 Proceso de llamada IP

Se envía la señal de información desde un equipo origen a un equipo destino a través de Internet cuando se trata de una red de telefonía IP pura. Cuando hablamos de una red telefónica híbrida, la llamada sería parcialmente a través de telefonía IP.

Posteriormente mediante un software, se traduce los números telefónicos o nombres de usuario a direcciones IP para poder direccionar a los diferentes usuarios con su respectiva red.

En los equipos o dispositivos terminales se realiza el proceso de digitalización de la voz, la cualse comprime, se fragmenta y se envía en paquetes generalmente a través de TCP/IP, no necesariamente por la misma ruta, pero sí hacia el mismo destino.

El equipo destino vuelve a armar en el orden correcto los paquetes que le llegan, los convierte a voz analógica para que pueda entender el usuario, y se envía a los auriculares del equipo.Al transmitir la voz en paquetes de datos se consume menos ancho de banda y se reduce los costos de interconexión al enviar la voz por canales de datos.

Todo esto proceso descrito se lo hace gracias a la arquitectura TCP/IP que permite transmitir los datos para lograr tener una comunicación de voz IP. La figura 1.3 explica de mejor manera la funcionalidad de TCP/IP en la telefonía IP:

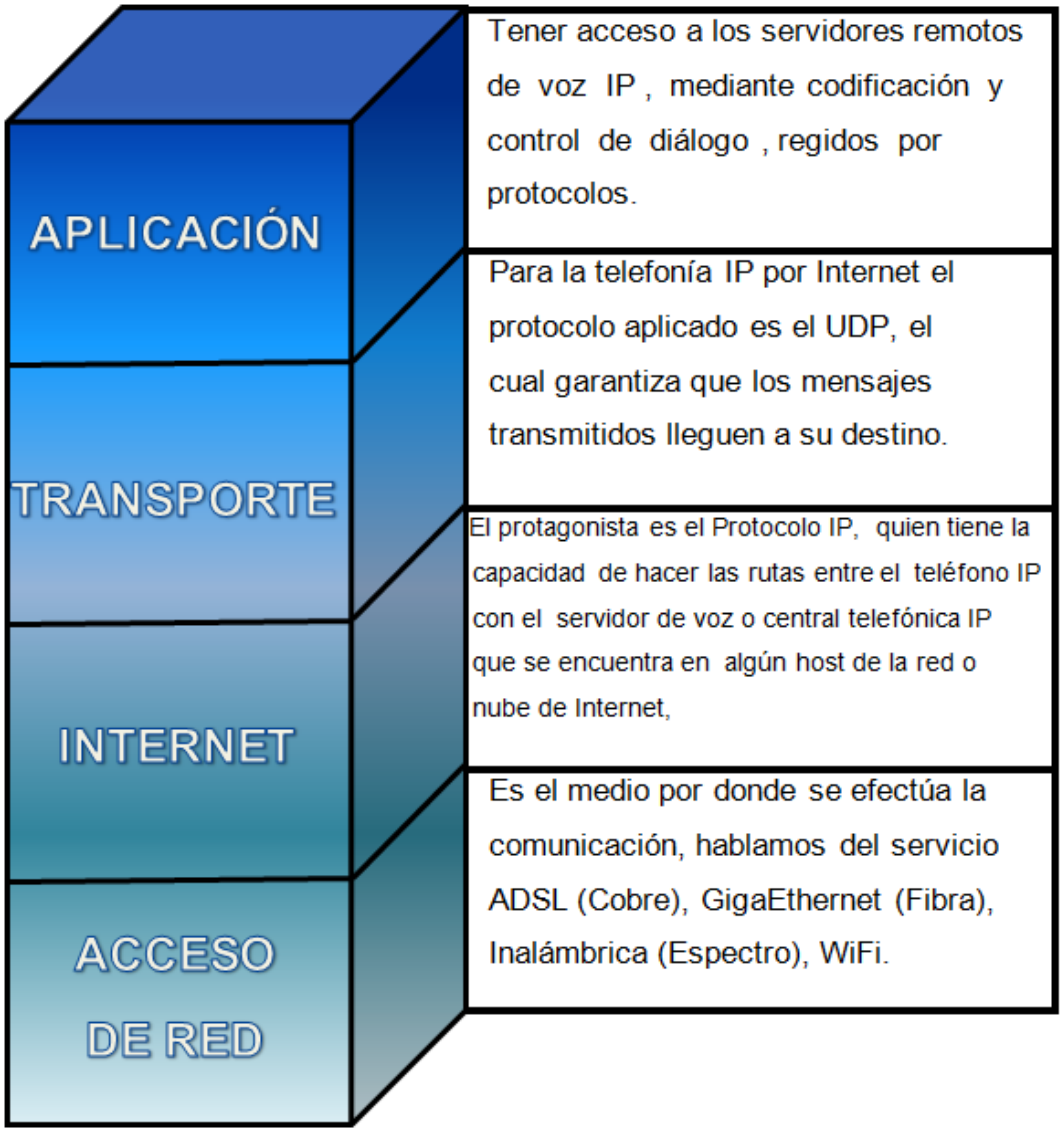

Figura 1.3 TCP/IP en telefonía IP

1.2.2.2 Tipos de llamadas en Telefonía IP. [2]

PC aPC: Para que se pueda establecer la comunicación en tiempo real entre los computadores, éstos deben tener instalada la misma aplicación encargada de gestionar la llamada telefónica. Este tipo de llamadas siempre son gratuitas. En la figura 1.4 se ilustra una llamada IP desde una PC hacia otra.

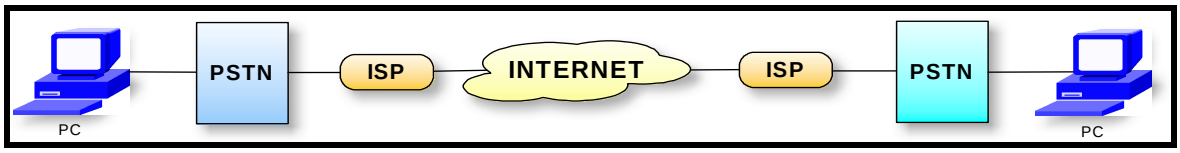

Figura 1.4 Llamadas de PC a PC

Teléfono a teléfono: En este tipo de comunicación tanto el origen como el destino deben conectarse con un Gateway, los cuales realizan una comunicación de datos a través de una red IP. En la figura 1.5 se ilustra una llamada IP desde un teléfono IP hacia otro.

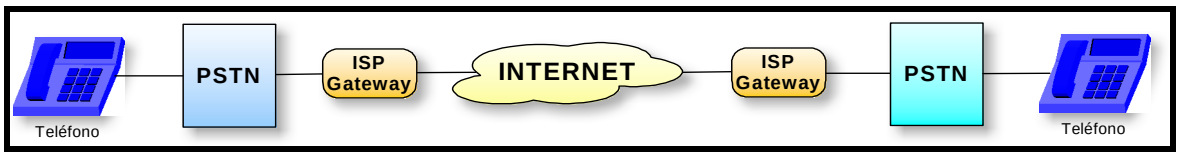

Figura 1.5 Llamada de teléfono a teléfono

PC a teléfono: Es necesario tener un solo Gateway conectado a Internet en un extremo de la comunicación y por otro lado a la PSTN para que digitalice, comprima y empaquete la voz. En la figura 1.6 se ilustra una llamada IP desde una PC hacia un teléfono IP.

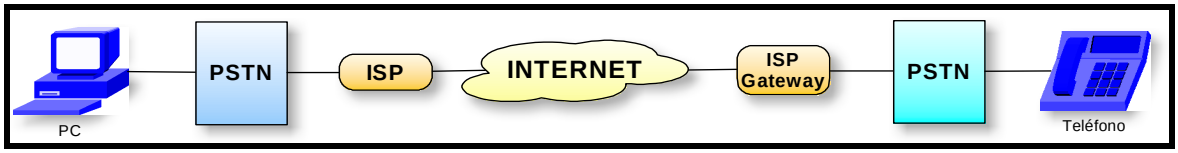

Figura 1.6 Llamada de PC a teléfono

1.3 SEÑALIZACIÓN EN TELEFONÍA [6] [7]

La señalización es el proceso por el cual se intercambia información de controlrelacionada con el establecimiento y la liberación de las comunicaciones y la gestión de la red. Las principales funciones de la señalización son:

- Control de tráfico

- Gestión de la red
- Acceso a base de datos

En la figura 1.7 se indica las principales funciones de la señalización en telefonía.

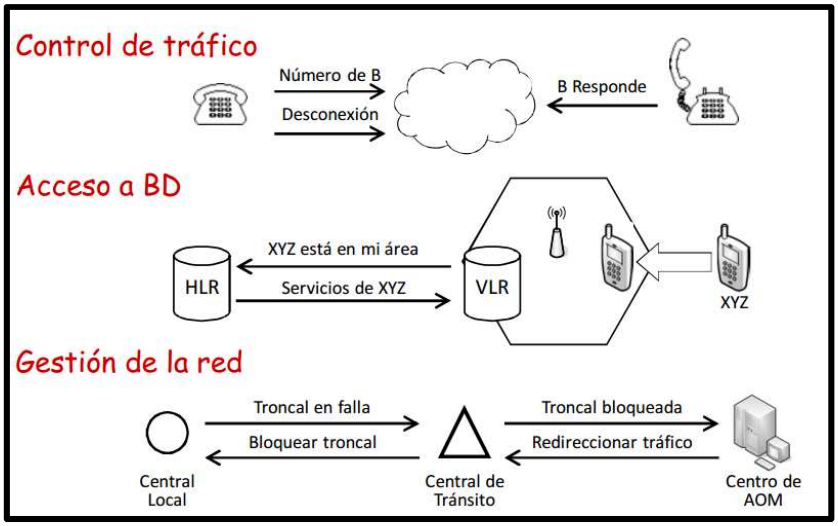

Figura 1.7 Funciones de la señalización [6]

1.3.1 TIPOS DE SEÑALIZACIÓN

1.3.1.1 Señalización de abonado [7]

Hace referencia al intercambio de un conjunto de señales entre el usuario y el centro de conmutación. Estas señales son las siguientes:

- **Supervisión o estado:** permite iniciar el establecimiento, mantenimiento y fin de la comunicación.
- **Dirección:** contiene información del destino.
- **Tarificación:** provee información sobre el costo de la llamada.
- **Información al usuario:** indica el estado de la llamada

1.3.1.2 Señalización entre centrales. [8]

Se refiere al intercambio de un conjunto de señales entre centrales. Existen dos diferentes maneras de enviar la señalización:

- Señalización asociada al canal.
- Señalización por canal común.

1.3.1.2.1 Señalización asociada al canal.

Esta expresión indica que la señalización se transmite por el mismo canal por donde se transmite el tráfico de voz. La señalización se transmite mediante un enlace PCM de 32 intervalos de tiempo para el estándar Europeo, en donde la señal de línea se envía por el intervalo 16 y las señales de registro se envían por los canales de tráfico de voz. En la figura 1.8 se puede observar a detalle este esquema de señalización.

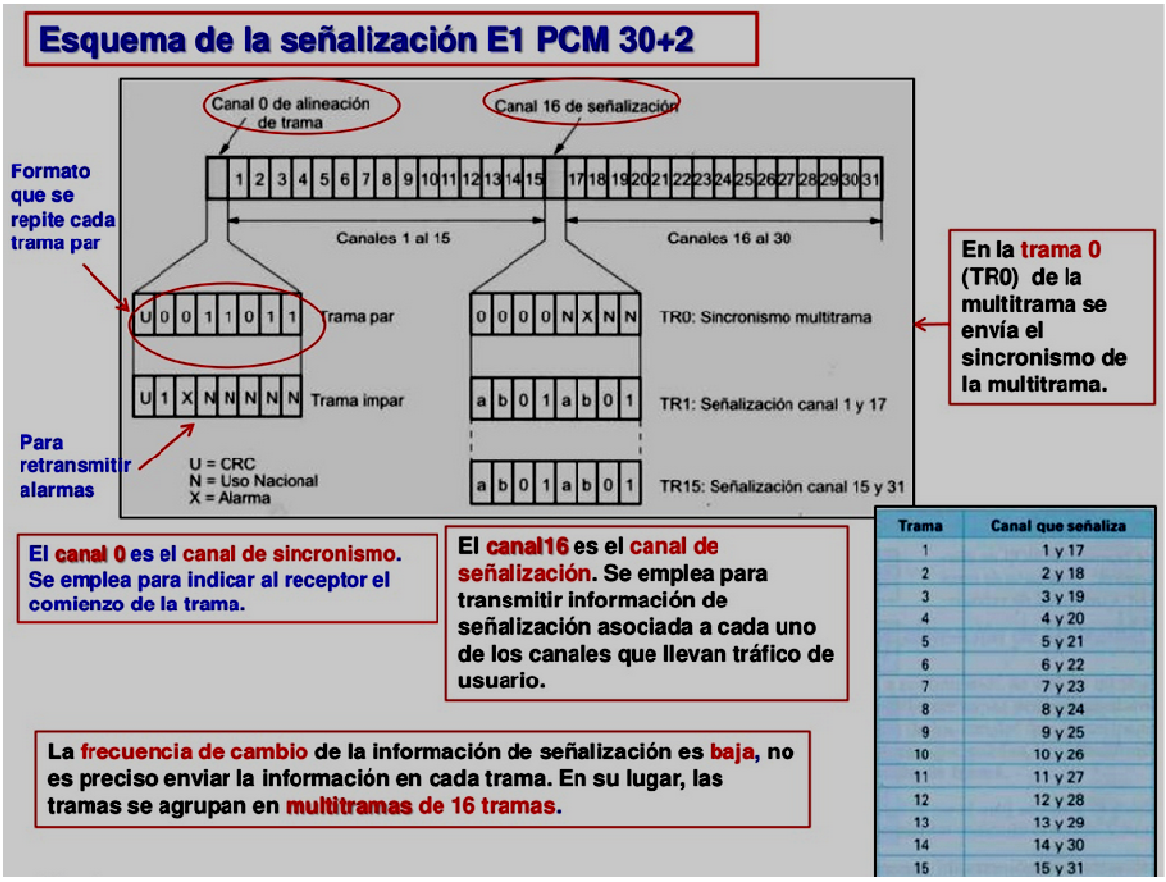

Figura 1.8 Esquema de señalización E1 [8]

1.3.1.2.2 Señalización por canal común. [7]

Por motivos de simplicidad y optimización de costos, se tomó la opción de crear un mecanismo de señalización separado de la red de tráfico de voz, dando lugar a la señalización por canal común que no es otra cosa que el uso de un mismo canal para enviar la señalización de varias comunicaciones separado del canal de voz. La señalización de canal común es más eficaz y flexible que la que se realiza

dentro del canal de voz dando mayor soporte a los requerimientos de las redes digitales de comunicación.

Desde ese entonces, se han desarrollado protocolos de señalización por canal común siendo el primeroelsistema de señalización N º 6 definido por la ITU-T, la cual posteriormente define SS7 como reemplazo de ES6 ya que no era apto para aplicarlo a sistemas digitales. Es así como SS7 sustituyo a todos los anteriores protocolos de señalización como son: ES6, además de sistemas de señalización por canal asociado como son: SS5, RI y R2.

Con los requerimientos actuales de telefonía IP, el sistema de señalización 7 tuvo que ser convertido a IP mediante los protocolos. Es decir que el momento que se realiza una llamada mediante telefonía IP, los protocolos SIGTRAN no reemplazan al SS7, solo lo complementa.

1.4 PROTOCOLOS DE SEÑALIZACIÓN.

A continuación se explicará a detalle los principales protocolos de señalización usados en telefonía.

1.4.1 PROTOCOLO SS7 [10][11]

1.4.1.1 Generalidades.

Este stack de protocolos fue desarrollado por AT&T desde el año 1975y fue catalogado como un estándar por la UIT-T en 1981.El sistema de señalización de canal común número 7 es un estándar que define el protocolo y la manera en la cual los elementos de la red telefónica pública conmutada intercambian información sobre una red digital para realizar el enrutamiento, establecimiento y control de llamadas.

Esta información es transportada en forma de mensajes. SS7 representa una red que transporta estos mensajes de señalización fuera de banda, es decir de forma independiente a la red que brinda propiamente el servicio.

1.4.1.2 Componentesde una red de señalización SS7. [11]

Una red de señalización SS7 está compuesta por puntos de señalización y enlaces de señalización.

1.4.1.2.1 Puntos de señalización [11]

Son de 3 diferentes tipos:

SSP (ServiceSwitching Point): Esunswitch de voz con capacidad de señalización 7. En los SSPs se originan y se terminan los mensajes de señalización. Son las centrales telefónicas que se encargan de la conmutación de las llamadas.

STP (Signal Transfer Point): Corresponde a los routers encargados de encaminar los mensajes de señalización hacia el destino correcto.

SCP (Signal Control Point): Concentran la inteligenciade la red SS7. Constituyen una base de datos de información de operación, mantenimiento y servicios suplementarios.

En la figura 1.9 se indica la manera como se relacionan los puntos de señalización anteriormente descritos.

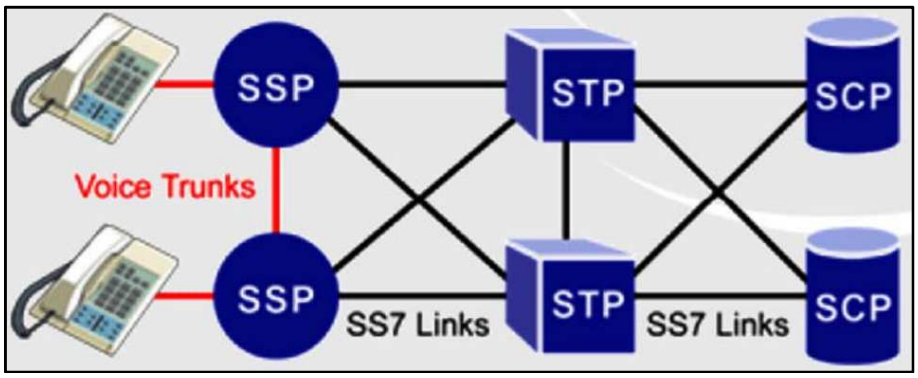

Figura 1.9 Puntos de señalización.

1.4.1.2.2 Enlaces de señalización:

Se refiere al tipo de conexiones que existen entre los puntos de señalización más no al tipo de líneas de transmisión que se utilizan. Son canales bidireccionales de 56 o 64 kbps.

1.4.1.3 Arquitectura de protocolos SS7 [10] [11]

La estructura distribuida en capas de la red SS7, se divide en cuatro niveles a conocer: físico, enlace de datos, red y usuario. Dentro de SS7, las capas más bajas como MTP1, MTP2 y MTP3 son propias del transporte a través de redes TDM y aparecen modificadas en otros modelos de transporte. Con lo cual, si en vez de usar TDM se usa Sigtran (Ethernet), toda la parte de MTP 1, 2 y 3 se sacarían, y solo se utiliza la capa de aplicación; que es la que tiene los mensajes de señalización. Por esta razón, el protocolo más importante es ISUP ubicado en la capa de aplicación.

En la figura 1.10 se puede observar la pila de protocolos que conforman la señalización SS7.

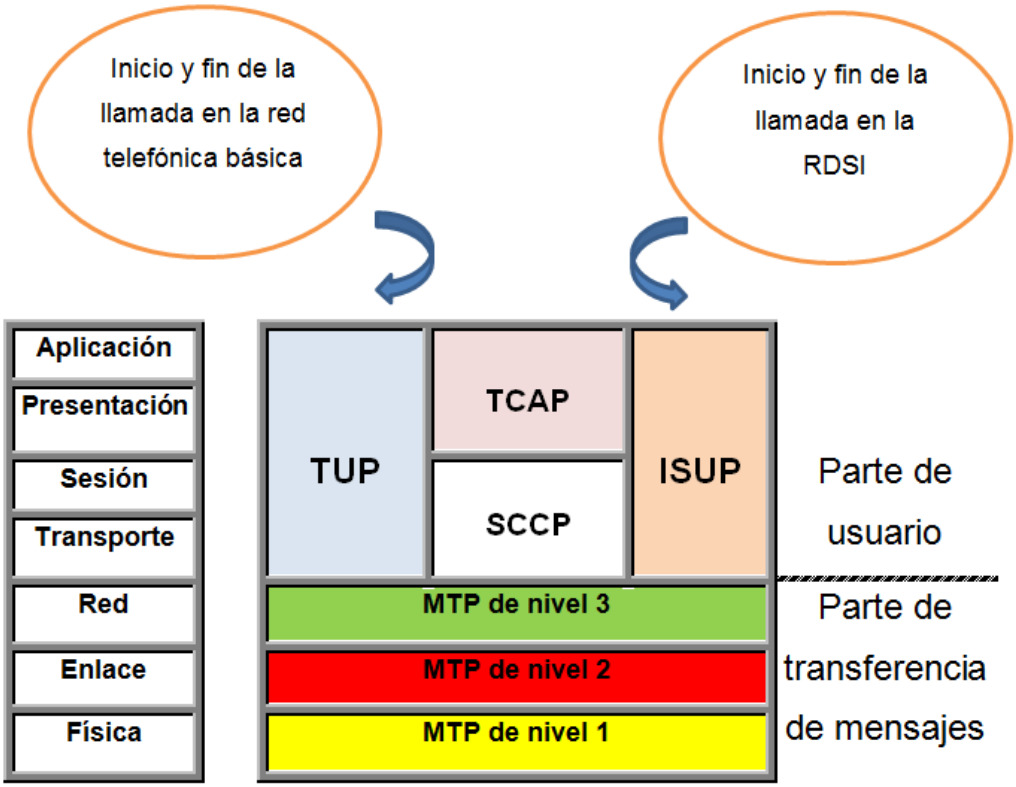

Figura 1.10Stack de protocolos SS7

MTP1: Corresponde a una capa típica TDM, es decir que consiste en un par de canales de transmisión digital con una velocidad de transmisión de 64 kbps. Transportan los datos SS7 entre dos puntos de señalización.

MTP2: Encargado de entregar los mensajes de señalización en forma ordenada y libre de errores de los mensajes de señalización. Sus principales funciones son:

- Detección y corrección de errores.
- Secuenciamiento de tramas de señalización
- Delimitación de tramas de señalización.
- Control de flujo.

MTP3: Se encarga del enrutamiento de los mensajes de señalización y de dar respuesta a problemas como congestión y falla en los enlaces.

SCCP: Facilita el transporte de mensajes orientados y no a conexión proveyendo de un mecanismo más dinámico para la transmisión de datos.

TCAP: Permite el intercambio de mensajes no relacionados con el circuito entre dos aplicaciones. Es responsable del manejo entre solicitudes y respuestas entre SSPs y SCPs.

TUP: Inicialmente se creó para el establecimiento y desconexión de llamadas. Fue reemplazado en su totalidad por ISUP.

ISUP: Responsable las funciones de establecimiento ygestión de las llamadas telefónicas en los troncales de la PSTN. Actualmente ISUP transporta la señalización tanto para terminales tradicionales como terminales tipo ISDN.

1.4.2 PROTOCOLO MEGACO/ H.248. [12] [13]

1.4.2.1 Generalidades.

MeGaCo (Media Gateway Control), creado por IETF, y H.248, creado por ITU-T, hacen referencia al mismo tipo de protocolo. Actualmente definido en el RFC 3525.

Este protocolo permite el intercambio de control entre MGC (Media Gateway Controller) y MG (MediaGateway) y de esta forma poder gestionar las llamadas entre redes.

1.4.2.2 Componentes que intervienen en sistema MEGACO. [13]

Controlador de Media Gateway (MGC): También conocido como agente de llamada. Se encarga de adaptar los medios, además realiza funciones específicas como traslación de direcciones, cancelación de eco entre otras.

Media Gateway (MG): Es el punto por donde sale o entra el tráfico telefónico desde o hacia la red telefónica convencional. Es decir que se encarga del mapeo de la señalización entre redes de paquetes y redes tradicionales.

En la figura 1.11 se puede observar los elementos que intervienen en MEGACO y la forma como se comunican.

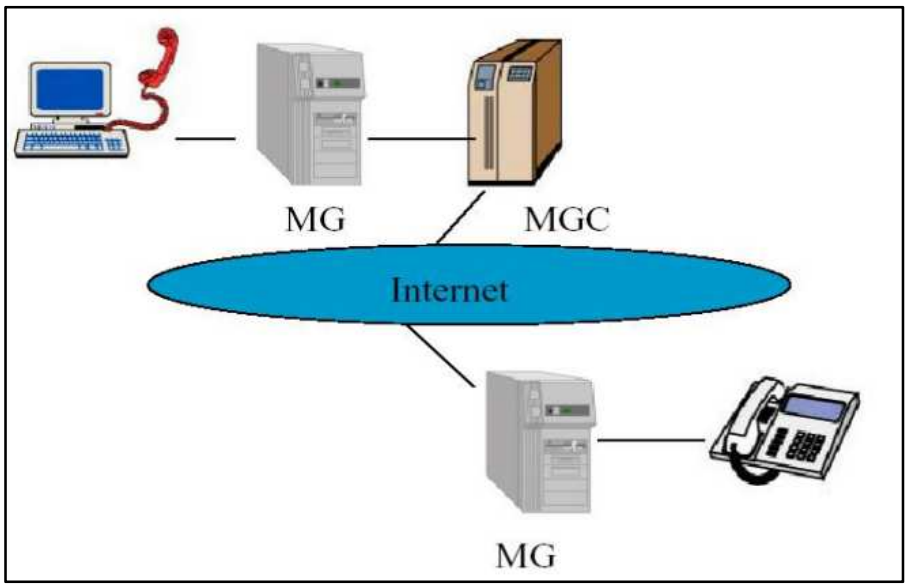

Figura 1.11 Componentes de MEGACO

1.4.2.3 Estructura del mensaje H.248/MEGACO [12] [13]

La estructura de un mensaje H.248/MEGACO consta de diferentes campos como se indica en la figura 1.12.

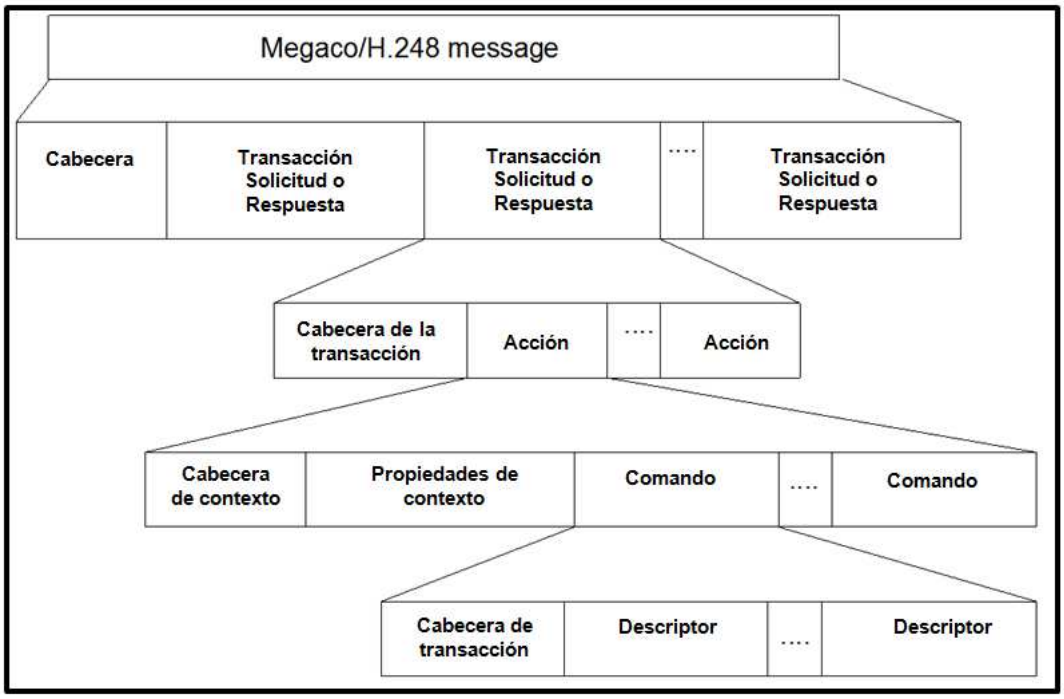

Figura 1.12 Estructura mensaje H.248/MEGACO

1.4.2.3.1 Transacciones en el mensaje [12][13]

Una transacción está constituida por una acción o varias de ellas. Una acción es un conjunto de instrucciones que se aplica a una circunstancia determinada.Una transacción es identificada por el campo Identificador de Transacción(Transaction ID) especificada por el origen, y es única en su ámbito.Las transacciones incluyen solicitudes y respuestas. Los comandos en una transacción son ejecutados en secuencia.

Transacciones como solicitudes:

Solicitud de transacción (TransactionRequest):

Es una petición hecha por el emisor; contiene una o variasacciones.Las instrucciones MEGACO seejecutande la siguiente forma:

TransactionRequest(TransactionId {

ContextID {Command , …, Command},

ContextID {Command, …, Command } })

Transacciones como respuestas:

Respuesta de Transacción (TransactionReply):

Es una respuesta del receptor hacia una solicitud de transacción. Debe haber una respuesta para cada transacción. Se ejecuta de la siguiente forma:

TransactionReply(TransactionID {

ContextID{ Response ...Response },

ContextID{ Response ...Response } })

Transacción Pendiente(TransactionPending):

Es una respuesta establecida por el receptor. Indica que una transacción está en procesamiento y que aún no termina. Limita al receptor para reenviar una solicitud de transacción.

TransactionPending (TransactionID { })

1.4.2.3.2 InstruccionesMEGACO [12]

Este protocolo define ocho tipos de instrucciones. En la tabla 1.3 se detalla las instrucciones con una breve explicación.

INSTRUCCIONES	DIRECCIÓN	DESCRIPCIÓN
Add	MGC→MG	Utilizado para agregar una Terminación a un Contexto. Si ninguna ContextID es especificada, un Contexto será generado y enseguida una Terminación será agregada a él.
Modify	MGC→MG	Utilizado para modificar las propiedades, eventos de señales de una Terminación.
Subtract	MGC→MG	Utilizado para remover una Terminación de un Contexto y retornar las estadísticas en la participación de la Terminación en el Contexto. El comando Subtract en la última Terminación en un Contexto excluye el Contexto.

Tabla 1.3 Instrucciones MeGaCo.

INSTRUCCIONES	DIRECCIÓN	DESCRIPCIÓN
Move	MGC→MG	Utilizado para mover una Terminación de un Contexto para otro.
AuditValue	MGC→MG	Utilizado para retornar el estado actual de las propiedades, eventos, señales y estadísticas de Terminaciones.
AuditCapabilities	MGC→MG	Utilizado para retornar una colecta de capacidades de Terminación.
Notify	MG→MGC	Utilizado para permitir que MG notifique el MGC sobre el evento detectado.
ServiceChange	MGC→MG	Utilizado para permitir que MG notifique el MGC de que una Terminación o grupo de Terminaciones están por ser retiradas o puestas en servicio. ServiceChange es también utilizada por MG para anunciar su disponibilidad para un MGC (registro), y utilizada para notificación de la paralización del MGC y switchover activo/standby.

(Continuación) Tabla 1.4 Instrucciones MeGaCo.

1.4.3 PROTOCOLO SIGTRAN. [14] [15] [16]

1.4.3.1 Generalidades. [15]

SIGTRAN se encuentra definido por la IETF en el RFC 2719 publicado en octubre de 1999. Es un conjunto de protocolos definido por la IETF el cual se encarga de transportar señalización de telefonía SS7 sobre redes IP. SIGTRAN describe la manera de presentar la información de SS7 sobre una red de transporte IP permitiendo una interoperabilidad entre redes IP de siguiente generación y redes SS7 ya existentes.

1.4.3.2 Componentes de la arquitectura de SIGTRAN. [14] [16]

Los protocolos SIGTRAN determinan los medios por los cuales se pueden transportar los mensajes de SS7 de una forma confiable sobre las redes IP Existen tres componentes de la arquitectura de SIGTRAN a saber:

- Capa de red: IP estándar como protocolo de red.
- Capa de transporte: Protocolo de transporte común para la capa protocolar de SS7. Soporta un conjunto común de funciones para el transporte confiable de la señalización
- Módulo de adaptación para emular las capas más bajas del protocolo. Existen varios protocolos de aplicación de señalización siendo entre los más importantes los siguientes: M2PA, M2UA, M3UA, SUA e IUA.

En la figura 1.13 se puede observar las capas correspondientes a la Arquitectura SIGTRAN.

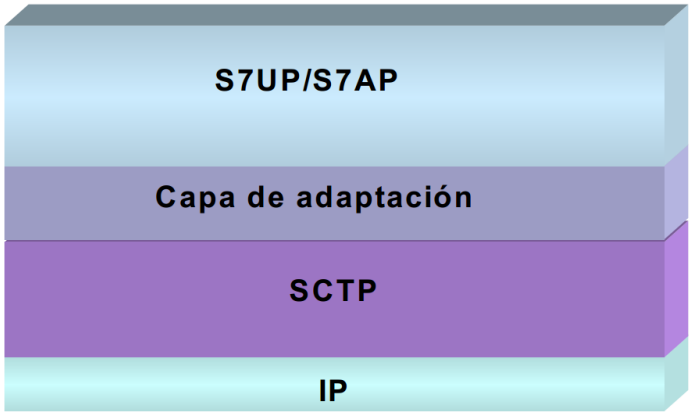

Figura 1.13 Arquitectura de SIGTRAN

1.4.3.2.1 Protocolo SCTP [9]

La capa encargada del transporte de la señalización se fundamenta en el protocolo SCTP (Stream Control TranmissionProtocol) en reemplazo de otros protocolos de transporte como son UDP, TCP e IPlos cuales se los definió para propósitos muy generales presentando limitaciones al momento de transportar señalización SS7.

El protocolo SCTP puede incluir dentro de un mismo mensaje SCTP a varios mensajes de señalización así como también los puede fragmentar. Es un protocolo orientado a mensajes, y detalla tramas de datos erstructurados.

El paquete SCTP está conformado por cabecera común y de un conjunto de bloques llamados chunks los cuales tienen en su estructura varios campos de información como se indica en la figura 1.14.

Bits	Bits 0 - 7	8 - 15	16 - 23	24 - 31
+0	Source port		Destination port	
32	Verification tag			
64	Checksum			
96	Chunk 1 type	Chunk 1 flags	Chunk 1 length	
128	Chunk 1 data			
...	...			
...	Chunk N type	Chunk N flags	Chunk N length	
...	Chunk N data			

Figura 1.14 Estructura paquete SCTP [9]

Estructura Cabecera común:

Puerto Origen (Source Port): Muestra el puerto origen de la asociación.

Puerto Destino (Destination Port): Muestra el puerto destino de la asociación.

Etiqueta de verificación (VerificationTag): Contiene un valor aleatorio que escoge independientemente tanto el cliente y el servidor. Discrimina entre asociaciones.

Verificación por redundancia cíclica (ChecksumCRC): Tiene como función chequear la totalidad de los datos del paquete.Adicionalmente, existen otros campos llamados fragmentos(chunks) que están conformados por los siguientes campos:

Tipo de fragmento (ChunkType): Contieneel tipo de fragmentoa enviar.

Bandera de fragmento (ChunkFlags): Definida por uno o más que contienen un determinado significado. Indica un tipo de bandera específica que posee cada fragmento. Depende del tipo de fragmento.

Longitud de fragmento (ChunkLength): Longitud del fragmento expresada en bytes.

Datos del fragmento (ChunkData): Corresponde a los datos enviados por el fragmento.

En la tabla 1.4se puede destacar algunos tipos de fragmentos como son:

TIPO	DESCRIPCIÓN
INIT	Inicia una asociación entre dos puntos terminales.
INIT ACK	Se encarga de reconocer la asociación.
SACK	Reconoce la recepción de chunks de datos.
HEARTBEAT	Se envía cuando no hay chunks que enviar.
HEARTBEAT ACK	Es una copia del HEARTBEAT pero en el otro sentido
ABORT	Termina una asociación de forma abrupta
SHUTDOWN	Finaliza las asociaciones de forma normal.
SHUTDOWN ACK	Se envía cuando todos los datos son reconocidos.
SHUTDOWN COMPLETE	Completa el fin de la asociación.
ERROR	Notifica errores
COOKIE ECHO	Se utiliza solo durante la iniciación de la asociación, luego de recibir un INIT ACK
COOKIE ACK	Puede ser multiplexado, es el primer chunk

Tabla 1.5 Tipos de fragmentos.

En el módulo de adaptación se encuentran diferentes protocolos como se puede observar en la figura 1.15

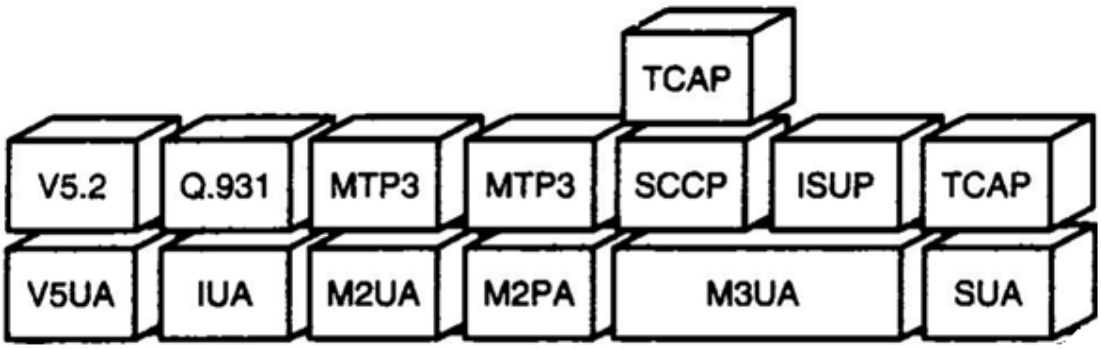

Figura 1.15 Protocolos en la capa de adaptación.

A continuación se describen los protocolos más importantes del módulo de adaptación en el stack de protocolos de SIGTRAN.

1.4.3.2.2 Protocolo M2PA [17][18][19]

M2PA son las siglas de MTP2-user peer-to-peer adaptation. Adapta el protocolo MTP-3, a SCTP entre pares. El usuario de M2PA es MTP-3 en ambos extremos de la comunicación. M2PA permite la comunicación directa a nivel de MTP-3 entre nodos SS7 y nodos IP como se puede ver en la figura 1.16.

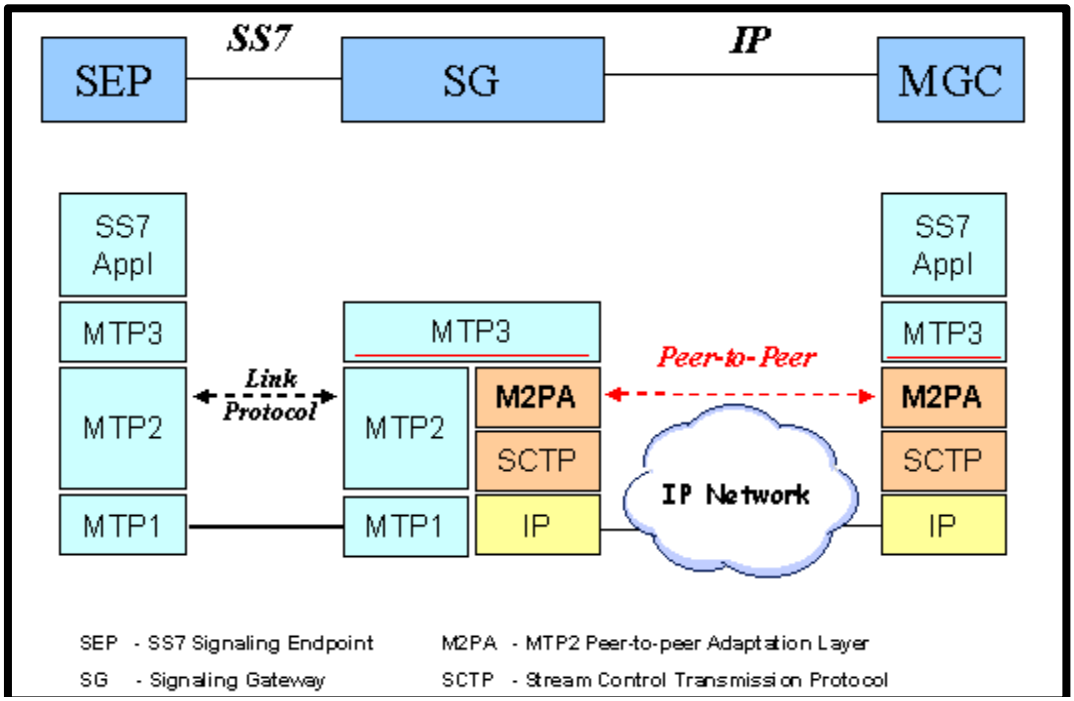

Figura 1.16 Comunicación mediante M2PA [18]

M2PA reemplaza en su totalidad a la capa MTP2 de SS7 ya que procesa las primitivas que requiere la capa MTP3.

Formato de los mensajes M2PA [17] [19]

Los mensajes M2PA cuentan con una cabecera común de 16 octetos donde constan los siguientes campos:

Versión: Contiene la versión de M2PA.

Campo disponible (Spare): Debe ser establecido todo en cero para el emisor e ignorado para el receptor.

Clase de mensajes: Para una clase válida se debe tener en este campo un valor decimal de 11. Cualquier otro valor indica una clase no válida.

Tipo de mensaje: Son de dos tipos: mensajes de usuario (campo con valor decimal de 1) y estado de enlace (valor decimal de 2).

Longitud del mensaje: Define la longitud del mensaje en octetos, incluida la cabecera común.

FSN (Forward SequenceNumber): Es el número de secuencia M2PA del mensaje de datos de usuario que se envió.

BSN (BackwardSequenceNumber): Es el FSN del último mensaje transmitido entre los pares

Los mensajes que se definen como datos de usuario cuentan adicionalmente con una cabecera de 2 octetos.En la figura 1.17 se presenta el formato de la cabecera M2PA.

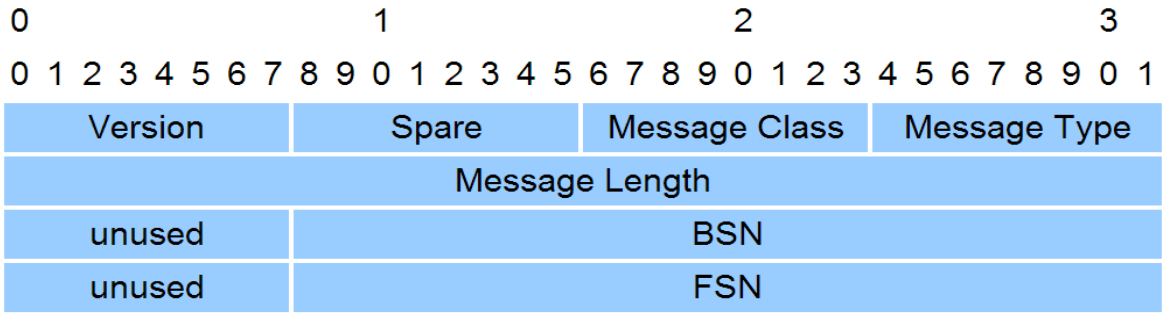

Figura 1.17 Cabecera M2PA[19]

1.4.3.2.3 Protocolo M2UA [19] [20][21]

M2UA es un protocolo definido para transportar los mensajes de SS7 MTP-2 entre una instancia MTP-2 en un SG y la instancia MTP-3 de un nodo de señalización basado en IP. Trabaja con un modelo cliente – servidor donde el nodo IP es el cliente y el SG es el servidor, por ello varios nodos IP con MTP3 pueden acceder a la red SS7 tradicional mediante los mismos enlaces MTP2 físicos.Esta arquitectura se usa cuando no hay muchos enlaces SS7 en un sitio en particular.

En la figura 1.18 se muestra un proceso de comunicación mediante el protocolo M2UA.

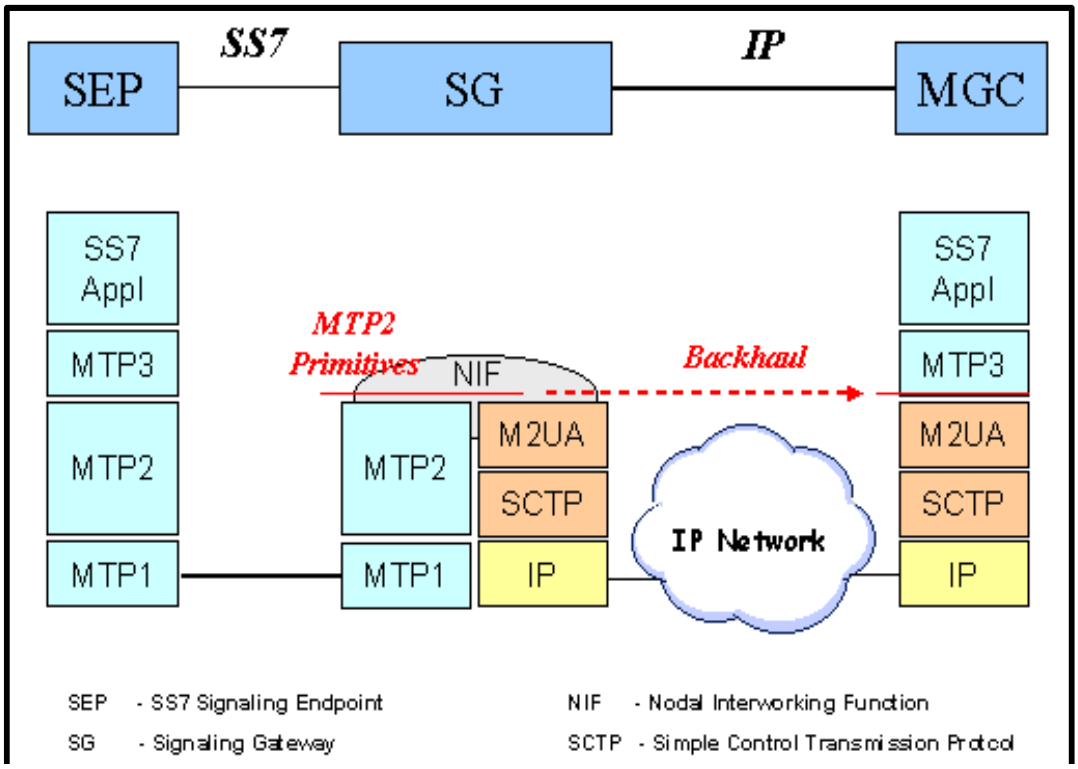

Figura 1.18 Proceso de comunicación con M2UA. [21]

Cuando la comunicación se establece directamente entre dos nodos de señalización basado en IP, M2UA actúa como un protocolo entre pares.

Formato de los mensajes M2UA [19] [20]

La cabecera común de los mensajes M2UA cuenta con los siguientes campos en su estructura como se observa en la figura 1.19.

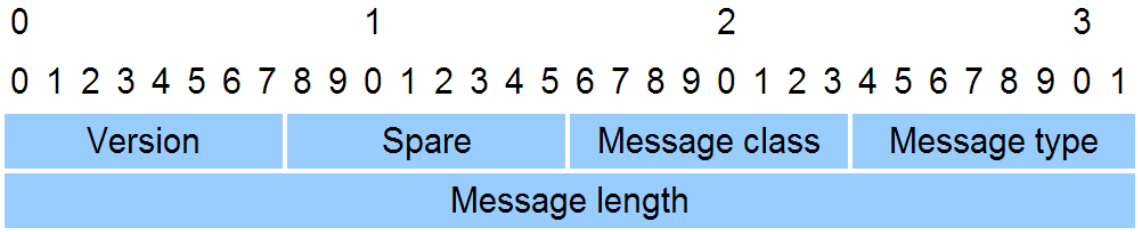

Figura 1.19 Cabecera Común M2UA [19]

Versión: Contiene la versión de M2UA. La versión soportada es 1.0

Campo disponible (Spare): Campo que debe establecerse en cero.

Clase de mensaje: Existen algunas clases de mensajes válidos. Es un campo que corresponde a un valor de 8 bits sin signo. En la tabla 1.5 se detalla las principales clases de mensajes:

Valor	Clase de mensaje
0	Mensaje de gestión MGMT
3	Mensaje de mantenimientodel estado del ASP
4	Mensajes del mantenimiento del tráfico ASP.
6	Mensajes de M2UA

Tabla 1.6 Clases de mensajes M2UA

Tipo de mensajes: Este campo contiene los diferentes tipos de mensajes para las clases de mensajes válidas como indica la tabla 1.6:

CLASE	TIPO	VALOR
Mensaje de gestión MGMT	Error	0
	Notificar	1
Mensaje de estado de mantenimiento del ASP	ASP up (UP)	1
	ASP down (DOWN)	2
	ASP up ACK (UP ACK)	4
	ASP down ACK (DOWN ACK)	5
Mensajes del mantenimiento del tráfico ASP.	ASP ACTIVE	1
	ASP INACTIVE	2
	ASP ACTIVE ACK	3
	ASP INACTIVE ACK	4

Tabla 1.7 Tipo de mensajes M2UA

CLASE	TIPO	VALOR
Mensaje de M2UA	Data	1
	Petición de establecimiento	2
	Confirmación de establecimiento	3
	Petición de liberación	4
	Confirmación de liberación	5
	Indicación de liberación	6
	Petición de Estado	7
	Confirmación de Estado	8
	Indicación de Estado	9
	Petición de recuperación de datos	10
	Confirmación de recuperación de datos	11
	Indicación de recuperación de datos	12
	Indicación de recuperación de datos completa	13
	Indicación de congestión	14
	ACK Datos	15

(Continuación) Tabla 1.6 Tipo de mensajes M2UA

Longitud de mensaje: Define la longitud del mensaje en octetos incluidos la cabecera así como también los bytes de relleno.

Los mensajes M2UA están compuestos de una cabecera común seguida de parámetros de longitud variable. Existen parámetros obligatorios los cuales deben

estar siempre antes que los parámetros opcionales dentro del mensaje. Estos parámetros tienen la estructura que se indica en la figura 1.20.

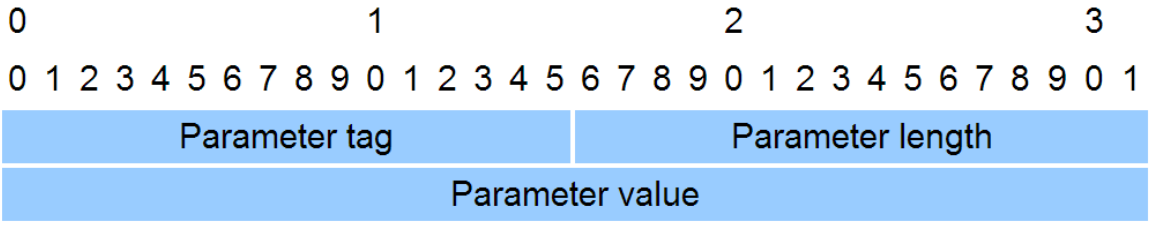

Figura 1.20 Formato de los parámetros de longitud variable M2UA [19]

Etiqueta de parámetro: Identifican los tipos de parámetros.Las etiquetas de parámetros más comúnmente utilizadas se describen en la tabla 1.7.

Parameter Value	Parameter Name
0 (0x00)	Reserved
1 (0x01)	Interface Identifier (Integer)
2 (0x02)	Unused
3 (0x03)	Interface Identifier (Text)
4 (0x04)	Info String
5 (0x05)	Unused
6 (0x06)	Unused
7 (0x07)	Diagnostic Information
8 (0x08)	Interface Identifier (Integer Range)
9 (0x09)	Heartbeat Data
10 (0x0a)	Unused
11 (0x0b)	Traffic Mode Type
12 (0x0c)	Error Code
13 (0x0d)	Status Type/Information
14 (0x0e)	Unused
15 (0x0f)	Unused
16 (0x10)	Unused
17 (0x11)	ASP Identifier
18 (0x12)	Unused
19 (0x13)	Correlation Id
18-255	Reserved

Tabla 1.8 Lista de etiquetas de parámetros M2UA

Longitud de parámetros: Indica el número de bytes que tiene los parámetros con sus respectivos campos.La longitud total de un parámetro siempre debe ser un múltiplo de 4 bytes. Caso contrario se rellena al final con bits establecidos en 0

Valor del parámetro: Contiene la información actual a ser transmitida por el parámetro.

1.4.3.2.4 Protocolo M3UA.[19][22][23]

M3UA es un protocolo que soporta el transporte de cualquier mensaje de señalización SS7 MTP3 sobre IP usando los servicios de SCTP. Es de funcionamiento similar a M2UA descrito anteriormente.

Es un protocolo descrito en el RFC 3332 el cual funcione entre el SG y el MGC brindado a éste último servicios de MTP3.

Esta arquitectura es más apropiada cuando hay una densidad de enlaces SS7 lo suficientemente alta para poder tener un SG autónomo; además cuando los enlaces son accesibles físicamente en un mismo punto. En la figura 1.21 se observa el transporte de una capa MTP3 utilizando M3UA.

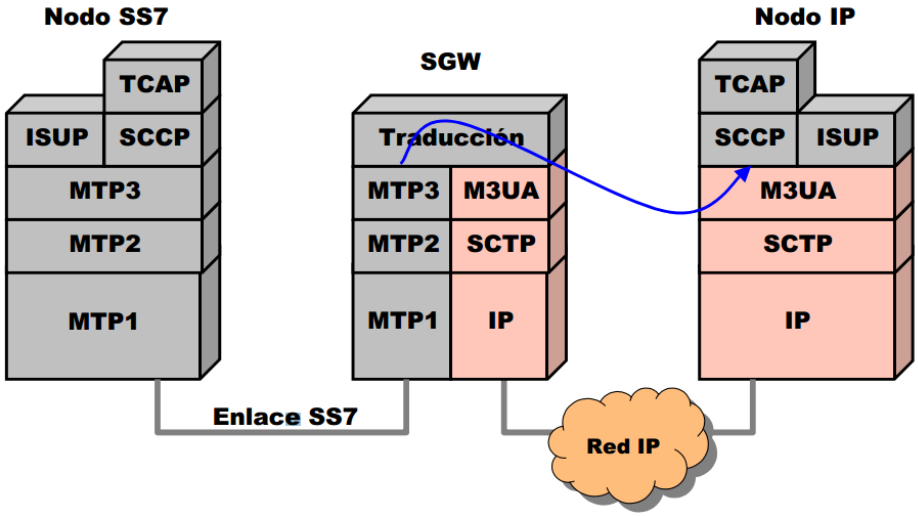

Figura 1.21Transporte con M3UA hacia una capa MTP3 remota [22]

Formato de los mensajes M3UA [23]

En la figura 1.22 se indica la estructura de un mensaje M3UA.

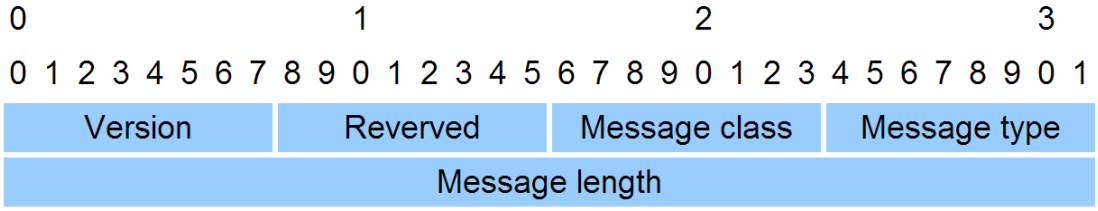

Figura 1.22 Estructura de la cabecera M3UA [19]

Versión: Contiene la versión de M3UA. La versión soportada es 1.0

Reservado: Todo este campo se debe establecer en cero.

Clase de mensaje: Las principales clases de mensajes pueden tomar diferentes valores como se indica en la tabla 1.8:

VALOR	CLASE DE MENSAJE
0	Gestión
1	Transferencia de mensajes
2	Gestión de red de señalización SS7
3	Mantenimiento del estado del ASP
4	Mantenimiento del tráfico ASP
9	Administración del enrutamiento de la clave

Tabla 1.9 Clases de mensaje M3UA

Tipo de mensaje: Este campo contiene los diferentes tipos de mensajes para las clases de mensajes válidas como indica la tabla 1.9.

CLASES	TIPOS	VALOR
Gestión	Error	0
	Notificación	1
Transferencia de mensajes	Datos útiles	1

Tabla 1.10 Tipos de mensajes M3UA

CLASES	TIPOS	VALOR
Gestión de red de señalización SS7	Destino no disponible	1
	Destino disponible	2
	Auditoría estado del destino	3
	Estado de la congestión del enlace SS7	4
	Destino no disponible de la parte de usuario	5
	Destino restringido	6
Mantenimiento del estado del ASP	ASP up	1
	ASP down	2
	Latencia	3
	ASP up ACK	4
	ASP down ACK	5
	Latencia ACK	6
Mantenimiento del tráfico ASP	ASP active	1
	ASP inactive	2
	ASP active ACK	3
	ASP inactive ACK	4
Administración del enrutamiento de la clave	Solicitud de registro	1
	Respuesta de registro	2
	Solicitud de cancelación de registro	3
	Respuesta de cancelación de registro	4

(Continuación) Tabla 1.9 Tipos de mensajes M3UA

Longitud del mensaje: Define la longitud del mensaje en octetos incluida la cabecera.

Los parámetros de longitud variable están a continuación de la cabecera y tiene la estructura que se muestra en la figura 1.23.

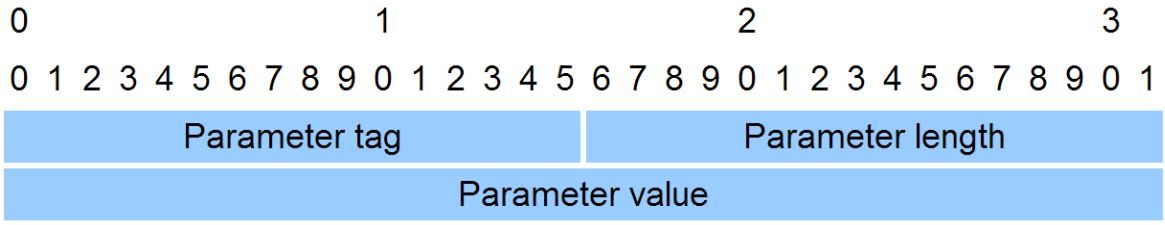

Figura 1.23 Estructura parámetros de longitud variable M3UA [19]

Etiqueta del parámetro: Identifican el tipo de parámetros.

En la tabla 1.10 se puede observar los diferentes tipos de parámetros:

0	Reserved
1	Network Appearance
2	Protocol Data 1
3	Protocol Data 2
4	Info String
5	Affected Destinations
6	Routing Context
7	Diagnostic Information
8	Heartbeat Data
9	User/Cause
10	Reason
11	Traffic Mode Type
12	Error Code
13	Status Type/ID
14	Congestion Indications
15	Concerned Destination
16	Routing Key
17	Registration Result
18	De-registration Result
19	Local_Routing Key Identifier
20	Destination Point Code
21	Service Indicators
22	Subsystem Numbers
23	Originating Point Code List
24	Circuit Range
25	Registration Results
26	De-registration Results

Tabla 1.11 Etiquetas de parámetros M3UA

Longitud del parámetro: Indica el tamaño del parámetro en bytes.

Valor: Indica el valor que se define para cada parámetro.

1.4.3.2.5 Protocolo IUA.[19][24]

Su nombre se deriva de ISDN Q.921-User AdaptationLayer. Este protocolo ha definido un módulo de adaptación para poder transportar mensajes establecidos en el interfaz usuario –red de una red digital de servicios integrados sobre IP.

Formato de mensajes IUA. [24]

Los mensajes IUA tienen en su estructura una cabecera seguida de parámetros de longitud variable como se indica a continuación.

Cabecera común.

La cabecera común de un mensaje IUA cuenta con la estructura que se presenta en la figura 1.24.

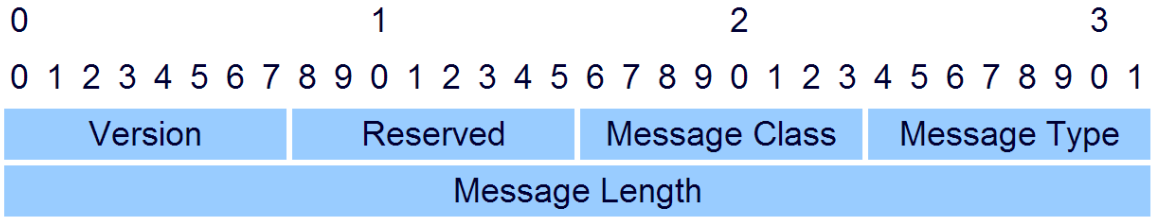

Figura 1.24 Estructura de la cabecera IUA [19]

Versión: Contiene la versión de IUA. La versión soportada es 1.0.

Reservado: Este campo tiene 8 bits, los cuales deben ser establecidos en cero.

Clase de mensaje: Las diferentes clases de mensaje con sus respectivos valores se detallan en la tabla 1.11.

VALOR	CLASES
0	Gestión
3	Mantenimiento del estado ASP
4	Mantenimiento del tráfico ASP
5	Transporte de los límites de las primitivas Q.921/Q.931
9-127	Reservado por la IETF
128-255	Reservado por la IETF

Tabla 1.12 Clases de mensajes IUA

Tipo de mensajes: Este campo contiene los diferentes tipos de mensajes para las clases de mensajes válidas como indica la tabla 1.12.

CLASES	TIPOS	VALOR
Transporte de los límites de las primitivas Q.921/Q.931	Reservado	0
	Solicitud de datos	1
	Indicación de datos	2
	Solicitud de unidad de datos	3
	Indicación de unidad de datos	4
	Solicitud de establecimiento	5
	Confirmación de establecimiento	6
	Indicación de establecimiento	7
	Solicitud de liberación	8
	Confirmación de liberación	9
	Indicación de liberación	10
	Reservado por la IETF	11 - 127
	Reservado por la IETF	128 - 255
Mantenimiento del estado ASP	Reservado	0
	ASP up	1
	ASP down	2
	Latencia	3
	ASP up ACK	4
	ASP down ACK	5
	Latencia ACK	6
	Reservado por la IETF	7-127
	Reservado por la IETF	128-255

Tabla 1.13 Tipos de mensajes IUA

CLASES	TIPOS	VALOR
Mantenimiento del tráfico ASP	Reservado	0
	ASP active	1
	ASP inactive	2
	ASP active ACK	3
	ASP inactive ACK	4
	Reservado por la IETF	5 -127
	Reservado por la IETF	128 - 255
Gestión	Error	0
	Notificación	1
	Pedido Estado TEI	2
	Confirmación Estado TEI	3
	Indicación Estado TEI	4
	Reservado por la IETF	5 -127
	Reservado por la IETF	128 - 255

(Continuación)Tabla 1.12 Tipos de mensajes IUA

Longitud de mensajes: Define la longitud del mensaje en octetos incluida la cabecera.

Parámetros de longitud variable.

A continuación de la cabecera se tiene los parámetros de longitud variable, la cual tienen la estructura que se muestra en la figura 1.25.

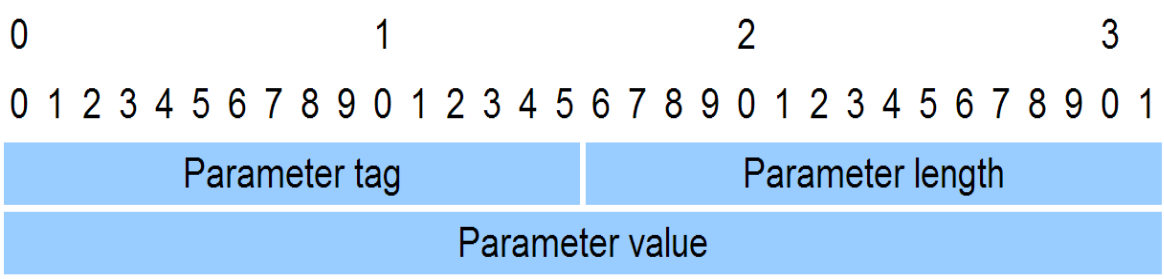

Figura 1.25 Estructura parámetros de longitud variable IUA [19]

Etiqueta del parámetro: Indica el tipo de parámetro.

A continuación se detalla las diferentes etiquetas de parámetros en la tabla 1.13.

Parameter Name	Parameter ID
Reserved	0x0000
Interface Identifier (integer)	0x0001
Not Used in IUA	0x0002
Interface Identifier (text)	0x0003
INFO String	0x0004
DLCI	0x0005
Not Used in IUA	0x0006
Diagnostic Information	0x0007
Interface Identifier Range	0x0008
Heartbeat Data	0x0009
Not Used in IUA	0x000a
Traffic Mode Type	0x000b
Error Code	0x000c
Status	0x000d
Protocol Data	0x000e
Release Reason	0x000f
TEI Status	0x0010
ASP Identifier	0x0011
Not Used in IUA	0x0012 - 0x003f

Tabla 1.14 Etiquetas de los parámetros IUA

Longitud del parámetro: Contiene el tamaño del parámetro en bytes incluyendo la etiqueta del parámetro, longitud del parámetro, y el valor del parámetro. No incluye bytes de relleno**.**

Valor del parámetro: Contiene la información actual a ser transferida en el parámetro.

1.4.3.2.6 Protocolo SUA.[19][25]

SUA son las siglas derivadas de SignallingConnection Control PartUserAdaptationLayer. Es un protocolo que provee los medios para que la parte de aplicación de un punto de señalización basado en IPpueda ser contactada por el SG. Múltiples nodos de señalización pueden ser contactados por un solo Gateway de señalización.

En la figura 1.26 se indica el proceso por el cual se transporta señalización mediante el protocolo SUA.

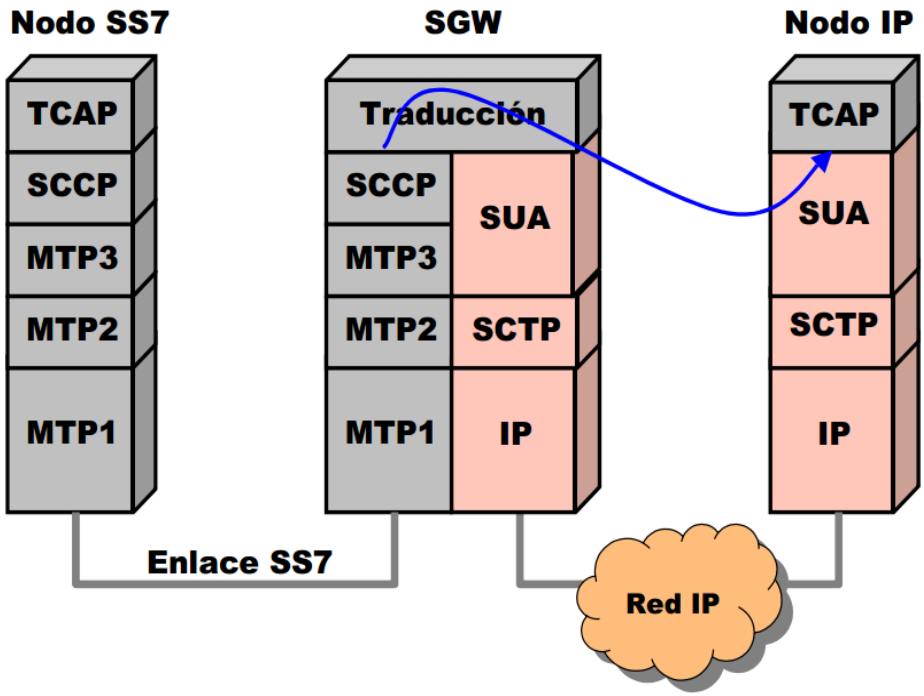

Figura 1.26 Transporte de señalización mediante SUA.

Formato de mensajes SUA. [25]

Los mensajes SUA tienen en su estructura una cabecera seguida de parámetros de longitud variable como se indica en la figura 1.27.

Cabecera común.

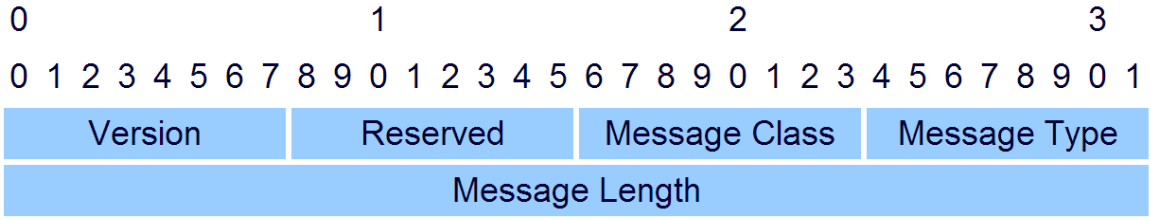

Figura 1.27 Cabecera común de mensajes SUA [19]

Versión: Contiene la versión de SUA. La versión soportada es 1.0.

Clase de mensajes: Para el protocolo SUA, están disponibles las clases de mensajes que se observan en la tabla 1.14

Valor	Clase
0	Gestión
2	Gestión de red de señalización SS7
3	Mantenimiento del estado ASP
4	Mantenimiento del tráfico ASP
7	Sin conexión
8	Mensajes orientados a conexión
9	Gestión del enrutamiento de claves.

Tabla 1.15 Clases de mensajes SUA.

Tipos de mensajes:

En la tabla 1.15 se observa los diferentes tipos de mensajes existentes en SUA.

Clases de mensaje	Tipos de mensajes	Valor
Gestión	Error	0
	Notificación	1
	Reservado por la IETF	2 – 127
	Reservado por la IETF	128 - 255
Gestión de red de señalización SS7	Reservado	0
	Destino no disponible	1
	Destino disponible	2
	Auditoría del estado del destino.	3
	Congestión de la red SS7	4
	Destino no disponible de la parte de usuario.	5
	Gestión de SCCP	6
	Reservado por la IETF	7-127
	Reservado por la IETF	128-255

Tabla 1.16 Tipos de mensajes SUA

Clases de mensaje	Tipos de mensajes	Valor
Mantenimiento del estado ASP	Reservado	0
	ASP up	1
	ASP down	2
	Latencia	3
	ASP up ACK	4
	ASP down ACK	5
	Latencia ACK	6
	Reservado por la IETF	7-255
Mantenimiento del tráfico ASP	Reservado	0
	ASP activo	1
	ASP inactivo	2
	ASP activo ACK	3
	ASP inactivo ACK	4
	Reservado por la IETF	5-255
	Reservado por la IETF	128-255
Sin conexión	Reservado	0
	Transferencia de datos sin conexión	1
	Respuesta de datos sin conexión	2
	Reservado por la IETF	3-127
	Reservado por la IETF	128-255

(Continuación) Tabla 1.15 Tipos de mensajes SUA

Clases de mensaje	Tipos de mensajes	Valor
Mensajes orientados a conexión	Reservado	0
	Solicitud de conexión	1
	Reconocimiento de conexión	2
	Rechazo de conexión	3
	Solicitud de liberación	4
	Liberación completa	5
	Confirmación de restablecimiento	6
	Solicitud de restablecimiento	7
	Transferencia de datos orientados a conexión	8
	Reconocimiento de datos orientados a conexión	9
	Error orientado a conexión	10
	Prueba de inactividad	11
	Reservado por la IETF	12-127
	Reservado por la IETF	128-255

(Continuación) Tabla 1.15 Tipos de mensajes SUA

Longitud del mensaje: Define el tamaño del mensaje IUA en octetos incluyendo la cabecera.

Parámetros de longitud variable.

A continuación de la cabecera se tiene los parámetros de longitud variable, la cual tienen la misma estructura que los protocolos SIGTRAN anteriormente descritos como indica la figura 1.28.

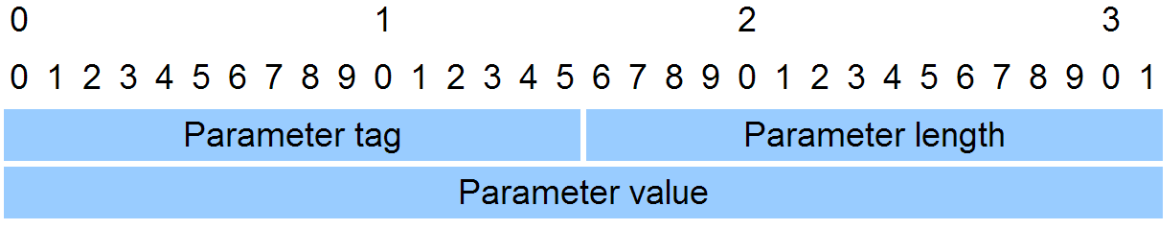

Figura 1.28 Estructura parámetros de longitud variable SUA [19]

Etiqueta del parámetro: Indica el tipo de parámetro.

Longitud del parámetro: Indica el tamaño del parámetro en bytes. No incluye bytes de relleno**.**

Valor del parámetro: Contiene la información actual a ser transferida en el parámetro.

1.4.4 PROTOCOLO SIP [26][27][28][29][30]

1.4.4.1 Generalidades.[26][29]

SIP es el acrónimo deProtocolo de Inicio de Sesiones; definido en el RFC 3261. Es un protocolo de señalización usado en telefonía y videoconferencia a través de internet o para comunicaciones que implican datos en tiempo real. SIP fue creado por IETF MMUSIC WorkingGroup para establecer, modificar y finalizar sesiones entre dos participantes así como también sesiones multicast. Este protocolo está basado en el Protocolo de Transporte de correo simple (SMTP) y en el Protocolo de Transferencia Hipertexto (HTTP).SIP es un protocolo fundamentado en el modelo cliente servidor y ubicado en la capa de aplicación de la arquitecturaTCP/IP, se usa para comunicaciones multimedia con otros protocolos como RSVP, RTP, SDP, entre otros.

El protocolo de Inicio de Sesiones es independiente de los protocolos de las capas inferiores, puede soportarse sobre TCP o UDP; además sobre IP, ATM, FrameRelay o X.25.

En la figura 1.29 se indica la ubicación del protocolo SIP dentro de la arquitectura TCP/IP.

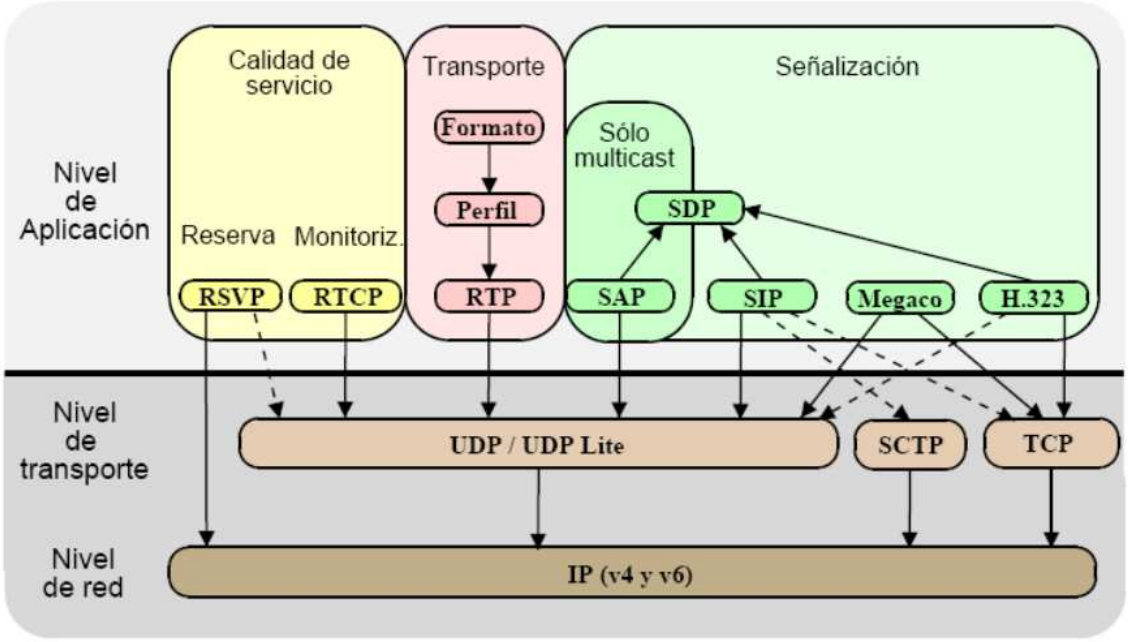

Figura 1.29 SIP dentro de la arquitectura TCP/IP [26]

1.4.4.2 Componentes de una red SIP [27][29][30]

Los componentes principales en la arquitectura SIP son: agentes de usuarios y servidores. Cada uno de estos componentes puede actuar en la comunicación como clientes (ente que inicia la solicitud) o como servidores (ente que responde la solicitud). Siendo así, los agentes de usuario se clasifican en:

- **Agentes de usuario clientes "UserAgentClient" (UAC):** Son entidades finales. Es una aplicación que envía una solicitud hacia la red IP.
- **Agentes de usuario servidores "UserAgent Server" (UAS):**Reciben una solicitud y originan una respuesta.

La figura 1.30 ilustra la comunicación existente entre UAC y UAS

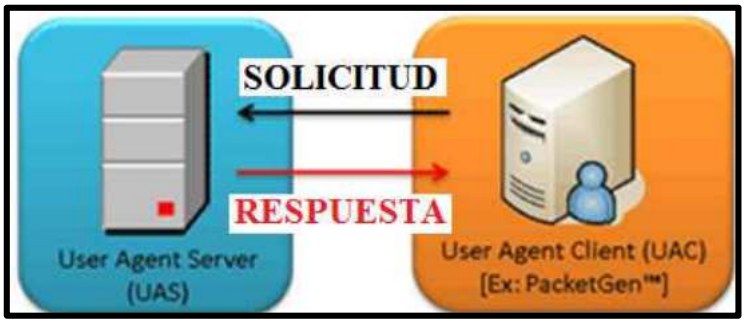

Figura 1.30 Comunicación entre UAC y UAS [30]

Los servidores SIP son aplicaciones o dispositivo que permite establecer y administrar cuentas SIP y el registro de Usuarios SIP mediante el almacenamiento de la dirección IP donde deben acceder para realizar la comunicación con este usuario [27]. Se clasifican de la siguiente manera:

- **Servidores proxy:** Es un componente intermediario que puede actuar como servidor al momento en que recibe las solicitudes SIP de un agente de usuario y devuelve una respuesta. Estos servidores en ocasiones debe reenviar la solicitud a otros servidores proxy actuando en estos términos como un cliente. Su principal función es la de enrutar las peticiones de sesión hacia el destino; en la mayoría de ocasiones una petición SIP debe pasar por varios servidores proxys para llegar a su destino mediante un servidor DNS para poder resolver las direcciones. En la figura 1.31 se indica el proceso de una llamada mediante un servidor proxy.

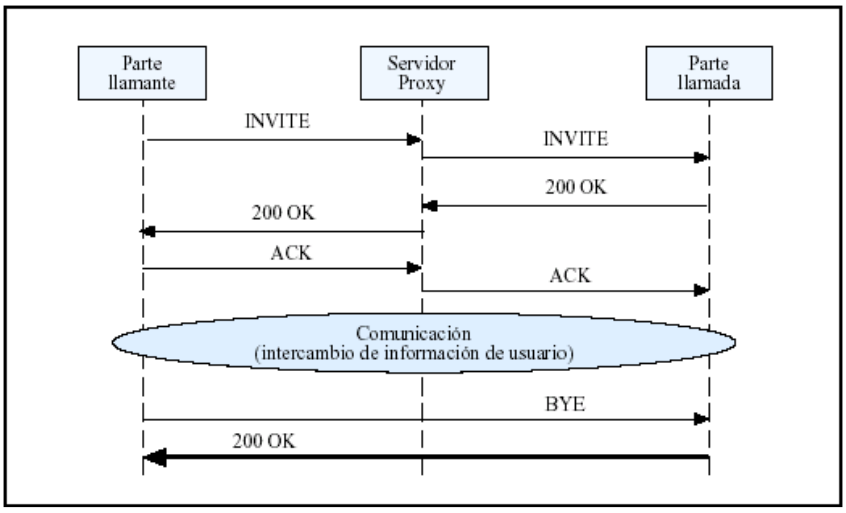

Figura 1.31 Comunicación SIP mediante servidor proxy. [28]

- **Servidores de redirección:** Acepta solicitudes de inicio de sesión(INVITE) y genera una respuesta a las mismas. En el caso en el que se conoce la dirección, este servidor mapea la dirección de destino y la proporciona al originante mediante un mensaje con código 3xx. Si no se conoce la dirección destino se la convierte a cero y se la devuelve al solicitante de la sesión mediante un mensaje con código 4xx.

En la figura 1.32 se indica el proceso de comunicación SIP mediante un servidor de redirección.

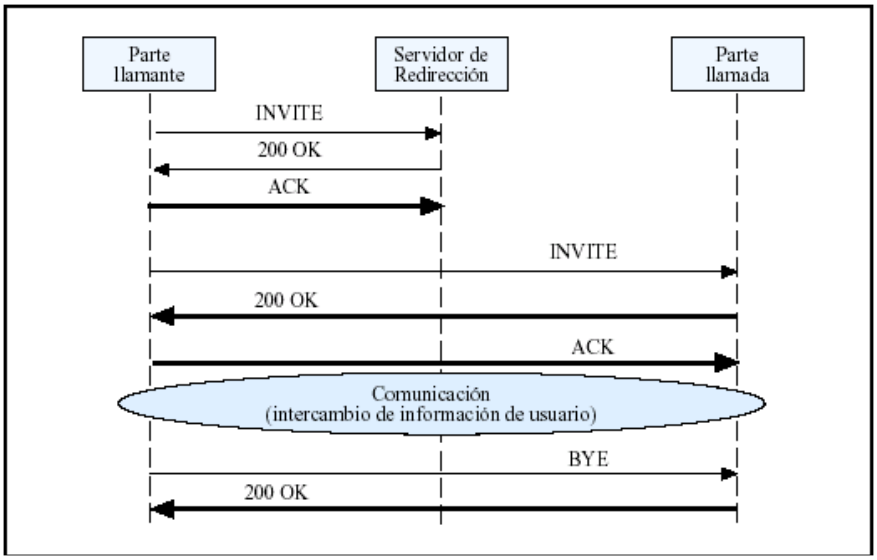

Figura 1.32 Comunicación SIP mediante servidor de redirección. [28]

- **Servidores de registro**Este servidor toma un mensaje de solicitud de registro y la ubica dentro de una base de datos en la cual están las ubicaciones de todos los agentes de usuario que se encuentran dentro del dominio.

  A este tipo de servidores también se los llama servidores de localización puesto que los servidores proxy y de redirección los usan para acceder a la localización del destino.

En la figura 1.33 se observa una comunicación mediante un servidor de registro.

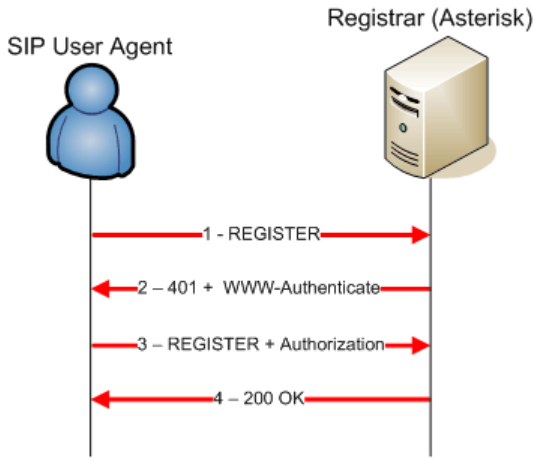

Figura 1.33 Comunicación mediante un servidor de registro

1.4.4.3 Mensajes SIP [26][29][30]

Los mensajes SIP tienen la forma de texto plano y utilizan una sintaxis muy parecida a la del protocolo HTTP. Estos mensajes pueden ser solicitudes o respuestas y su formato se lo detallaa continuación para cada uno de estos tipos.

1.4.4.3.1 Estructura de los mensajes SIP.[26][29][30]

La estructura general que presenta un mensaje SIP contiene las siguientes partes como se indica en la figura 1.34.

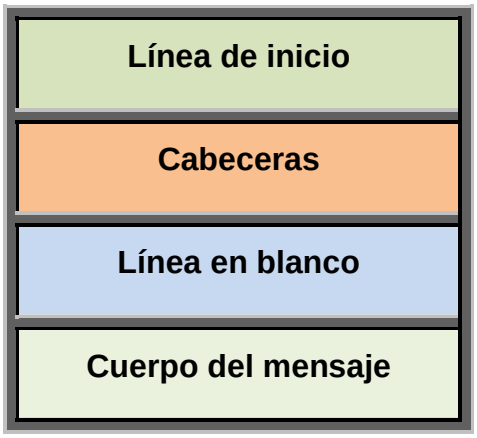

Figura 1.34 Formato mensajes SIP

Línea de inicio.

Es el comienzo de cualquier mensaje SIP. Esta línea está definida para mensajes de solicitud (línea de solicitud) y para mensajes de respuesta (línea de estado).

Mensajes de solicitud. [29]

Línea de solicitud: Contiene los siguientes campos como se indica en la figura 1.35.

Método	SP	Request - Url	SP	Versión del protocolo	CRLF

Figura 1.35 Estructura de línea de solicitud de mensajes SIP

Método: Detalla la acción que se quiere efectuar. Existen 6 diferentes tipos de métodos que se detallan en la tabla 1.16.

Método	Descripción
REGISTER	Petición de registro.
INVITE	Inicio de una sesión.
CANCEL	Cancela una solicitud de llamada incompleta.
BYE	Finalización de sesión.
ACK	Confirmación de la recepción de un INVITE.
OPTION	Consulta sobre especificaciones del receptor

Tabla 1.17 Métodos de un mensaje de solicitud SIP

*SP:*es un carácter simple que se lo usa como separación.

Request – Url: Indica el usuario al cual se envía la petición. Es decir contiene el SIP URL del host al cual está destinada la solicitud.

Un SIP URL contiene la información suficiente para iniciar y mantener una comunicación SIP. Un SIP URI no es otra cosa que el número telefónico SIP de un usuario y tiene el siguiente formato:

SIP_URI= SIP: usuario@equipo:puerto

En donde el usuario puede ser un nombre o un número telefónico mientras que el equipo puede ser un dominio o una dirección IP. El puerto que usualmente se utiliza es el 5060 tanto para UDP como para TCP.

*Versión del Protocolo:*La versión del protocolo SIP en uso es la SIP/2.0.

CRLF: Se compone de un carrierreturn + line feed. Es el carácter insertado al presionar la tecla enter del computador.

Mensaje de respuesta. [29]

Línea de estado: Contiene los siguientes campos como se indica en la figura 1.36

Versión del protocolo	SP	Status code	SP	Reason- Phrase	CRLF

Figura 1.36 Estructura de línea de estado de mensajes SIP

Versión del protocolo: La versión del protocolo SIP en uso es la SIP/2.0.

*SP:*es un carácter simple que se lo usa como separación.

Status code: Como resultado de una solicitud, se genera un entero de tres dígitos en donde el primer dígito representa la clase de respuesta hacia un pedido. En la tabla 1.17 se indica los diferentes códigos de estado para un mensaje de respuesta SIP.

Prefijo del código	Función	Ejemplos
1xx	Provisional, solicitud recibida	100: tratando.
		180: Timbrando.
		181: Llamada está siendo remitida.
		182: En cola.
		183: Progreso de la sesión.
2xx	Solicitud aceptada exitosamente	200: OK. Solicitud con éxito.
3xx	Solicitud redireccionada	300: Múltiples opciones.
		301:Movido permanentemente.
		302:Movido temporalmente.
		305: Uso de un proxy.
		380: Servicio alternativo.

Tabla 1.18 Códigos de estado de un mensaje de respuesta SIP

Prefijo del código	Función	Ejemplos
4xx	Solicitud con errores del cliente	400: Solicitud incorrecta.
		401: No autorizado.
		404: No encontrado.
		405: Método no permitido.
		408: Pedido fuera de tiempo.
		480: No disponible temporalmente.
		484: Dirección incompleta
		491: Solicitud pendiente.
		493: Indescifrable.
5xx	Fallas del servidor	500: Error del servidor interno.
		501: No implementado.
		502: Gateway incorrecto.
		503: Servicio no disponible.
		504: Servidor fuera de tiempo.
		505: Versión no soportada.
6xx	Fallas globales	600: Ocupado en todas partes.
		603: Declinación
		604: No existe en ningún lugar.
		606: No aceptable.

(Continuación) Tabla 1.17 Códigos de estado de un mensaje de respuesta SIP

*Reason-Phrase:*Describe de una forma textual y corta el código de estado.

CRLF: Se compone de un carrierreturn + line feed. Es el carácter insertado al presionar la tecla enter del computador.

Cabeceras de mensajes SIP. [29] [30]

Dentro de los campos de cabecera se encuentra información relacionada con la sesión como es: origen de la llamada, tipo de mensaje, trayectoria del mensaje entre otras características. Existen 47 tipos diferentes de cabecera definidos para el protocolo SIP agrupados en cuatro categorías como se indica en la tabla 1.18.

Cabeceras Generales	Cabeceras de Entidad	Cabeceras de solicitud	Cabeceras de respuesta
Call – ID	Allow	Accept	Proxy - Authenticate
Contact	Content Encoding	AcceptEncoding	Server
Cseq	Content Length	AcceptLanguaje	Unsupported
Date	Content Type	AcceptContact	Warning
Encryption	Content Disposition	Authorization	WWW-Authenticate
From	Expires	Hide	Rseq
Organization	MIME- Version	In-Reply -To	
RetryAfter		Max - Forwards	
Subject		Priority	
Timestamp		Proxy-Authorization	
To		Proxy - Require	
UserAgent		Record-Route	
Via		Reject - Contact	
		Request-Disposition	
		Require	
		Response - Key	
		Route	

Tabla 1.19 Cabeceras del mensaje SIP

Dentro de estos tipos de cabecera podemos detallar como más importantes a los siguientes:[30]

Identificador de llamada (Call-ID): Es el identificador único de una llamada.

Vía (Via): Identifica el tipo de transporte que se usó para el envío. Muestra la ruta de la solicitud.

De (From): Muestra la dirección del origen de la llamada.

Para (To): Muestra la dirección del destino de la llamada.

Contacto (Contact): Indica la ruta directa para contactarse con el usuario que realiza la petición.

Longitud del contenido (Content Length): Indica la cantidad de bytes del cuerpo del mensaje. Si no hay información este parámetro debe ser seteado en 0.

Tipo de contenido (Content-Type): Este parámetro indica el tipo de información contenida en el cuerpo del mensaje.

Comando de secuencia (Cseq): Es un comando de secuencia que identifica la transacción.

Agente de usuario (Useragent): Muestra el agente de usuario cliente que realiza la transacción.

Métodos soportados (Allow): Muestra los métodos soportados por el agente de usuario. Si este parámetro no está presente en la cabecera es porque el agente de usuario no proveyó ningún método.

Número máximo de saltos (Max Forwards): Limita la cantidad de saltos que una petición puede realizar.

Cuerpo del mensaje SIP. [29][30]

El cuerpo del mensaje SIP se usa para describir la sesión que va a comenzar; también se lo llama carga útil y puntualiza algunas características específicas como son: versión del códec (normalmente el estructurado en SDP) de video y audio así como también frecuencias de muestreo.

Los principales parámetros de este campo son:

Versión SDP (v): En este parámetro se especifica la versión del protocolo SDP.

Propietario/Creador, Sesión Id (o): Muestra el identificador de la sesión, la IP y el propietario.

Información de conexión (c): Define la IP donde se deben enviar los datos de audio.

Descripción del tiempo (t): Corresponde al tiempo que lleva activo el flujo de datos de audio.

Descripción del medio: Detalla los códecs soportados por el agente de usuario clienteque inició la comunicación.Para identificar a los códecs se utilizan valores preestablecidos estándar: 8 G.711A , 0 G711U, 4 G.723, etc.

Este campo es opcional, está información interesa únicamente a los agentes de usuario pero no así a los servidores los cuales solo necesitan tener información de la línea de inicio y de las cabeceras para poder enrutar los mensajes SIP.

En la figura 1.37 se presenta un ejemplo de mensaje SIP de solicitud.

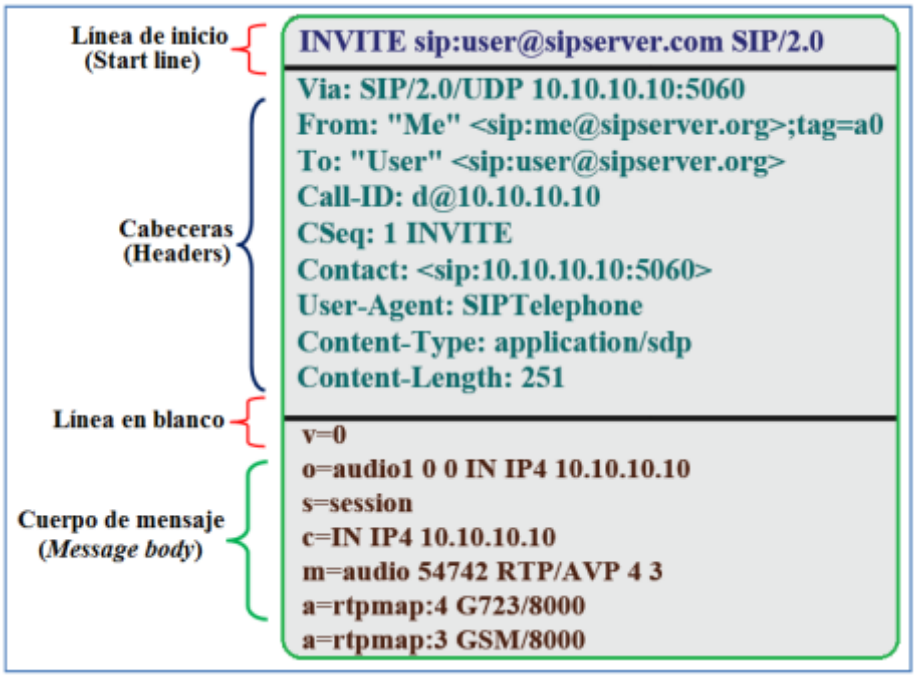

Figura 1.37 Ejemplo de un mensaje de solicitud SIP

En la figura 1.38 se presenta un ejemplo de mensaje SIP de respuesta.

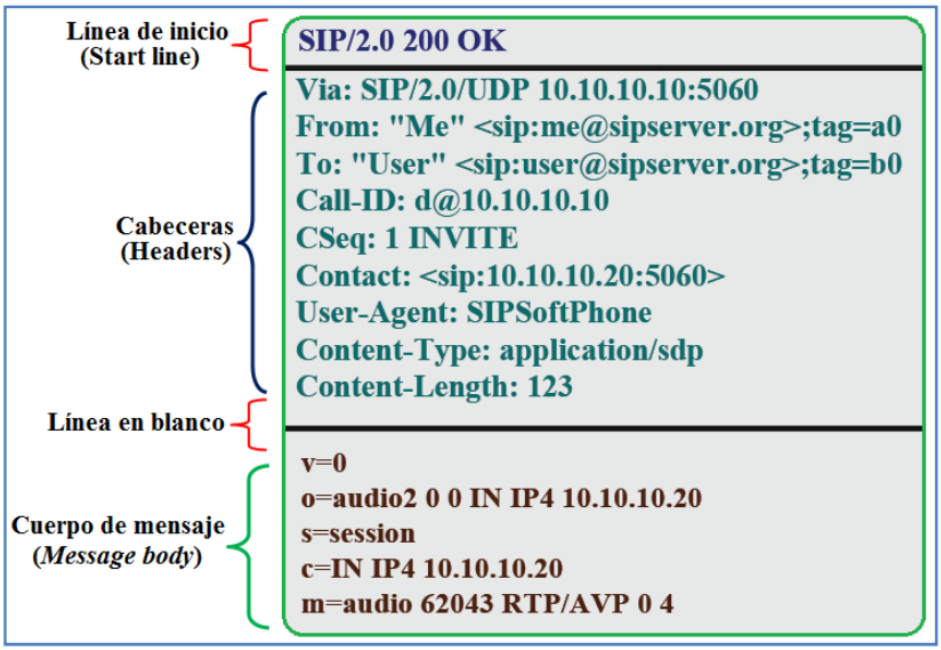

Figura 1.38 Ejemplo de un mensaje de respuesta SIP

CAPÍTULO 2.

MÉTODOS DE CONTROL DE FRAUDE EN EL TRÁFICO TELEFÓNICO.

2.1 INTRODUCCIÓN.

El fraude ha tenido sus inicios mucho tiempo atrás dentro de la sociedad y se ha desarrollado en diversos campos: financieros, legales, sociales, informáticos y tecnológicos. Dentro de las telecomunicaciones el fraude se ha desarrollado con gran importancia e impacto hacia las empresas que prestan estos servicios ya que todas ellas son vulnerables al fraude.

En el sector de las telecomunicaciones, desde un inicio se han ideado muchas formas desde las más simples hasta técnicas complejas para poder obtener beneficios de forma ilegal del servicio mencionado y brindado por empresas legalmente establecidas, las cuales sufren cuantiosas pérdidas a causa de este mal.

Por esta razón es de suma importancia dar el debido tratamiento y gestión a este tema para poderlo controlar. Para ello se analizan diferentes aspectos relacionados con el fraude a fin de entenderlo de una forma más detallada y poder determinar procesos de detección, corrección y prevención del mismo.

2.2 CONCEPTO DE FRAUDE.

2.2.1 FRAUDE.[31]

Este término define un abuso de confianza o engaño hacia un tercero, sea éste una persona natural o una empresa. Los fraudes pueden ser realizados tanto por individuos como por empresas. Como característica general, los fraudesinciden en corrupción, mentiras, uso indebido de recursos, alteración de información, etc.

2.2.2 FRAUDE EN TELECOMUNICACIONES [34]

En telecomunicaciones, el fraude se determina por conductas ilegítimas que perjudican intereses de abonados y usuarios como cobertura y calidad de

servicio. El fraude es el uso deshonesto de servicios de telecomunicaciones donde la persona que lo comete no tiene la intención de pagar por los servicios utilizados.

Existen varios factores que impulsan el cometer fraude en las telecomunicaciones como son: gran avance tecnológico, movilidad de los servicios, convergencia tecnológica determinada por la interconexión de redes mediante la red Internet entre otros.

En la actualidad es de gran importancia el uso de herramientas que permitan controlar el tráfico telefónico para poder identificar conductas inusuales por parte de los suscriptores que puedan reflejar potenciales usos indebidos de los servicios o casos de fraude dentro de las telecomunicaciones que posteriormente se traducen en pérdidas económicas para las empresas.

En el sector de las telecomunicaciones, es necesario tratar y gestionar al fraude con la debida importancia, puesto que este hecho produce pérdidas de alrededor del 4.8% del total de ingresos obtenidos por las empresas que brindan servicios de telecomunicaciones. Dichas empresas continuamente buscan implementar a sus procesos de gestión de fraude diferentes métodos para su detección y su posterior solución.

2.3 TRIÁNGULO DEL FRAUDE. [32]

Existen tres elementos que intervienen en el acto de fraude y son:

Motivación: Es el incentivo o estímulo para realizar un acto fraudulento, es decir la razón o causa.

Justificación: Es el acto que realiza el defraudador en el que trata de argumentar a sí mismo que tiene razones válidas para realizar el fraude.

Oportunidad: Cuando la persona fraudulenta percibe un escenario con circunstancias favorables y una probabilidad alta de poder cometer el fraude sin el riesgo de ser descubierta.

En la figura 2.1 se indica los elementos que conforman el triángulo de fraude.

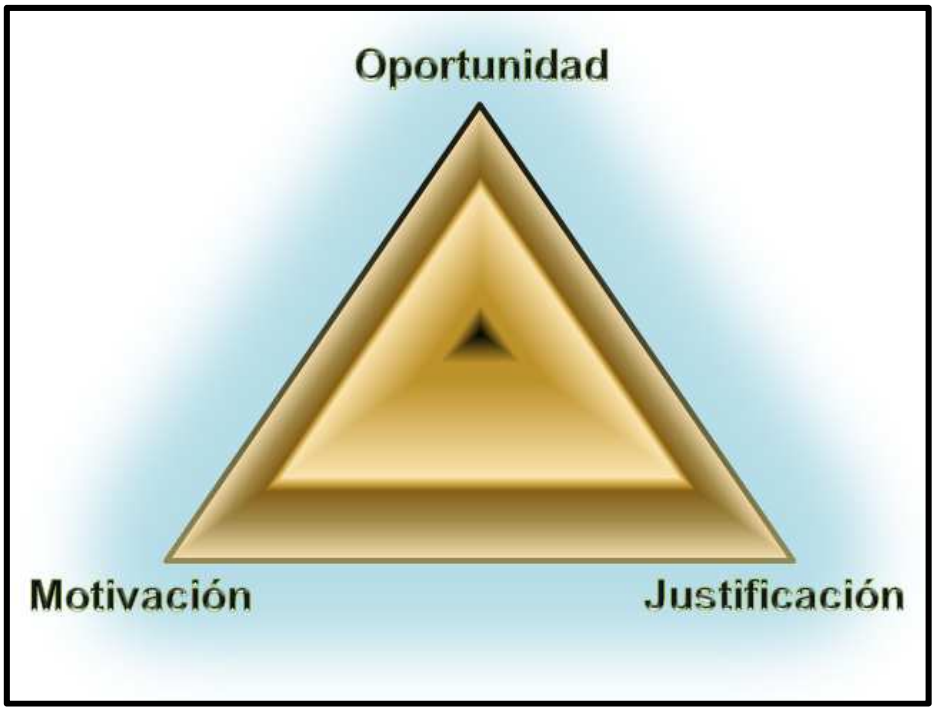

Figura 2.1 Triángulo del Fraude

2.4 CONTROL DE FRAUDE. [31]

Para lograr tener un control de fraude eficaz se necesita implementar cuatro procesos:

Prevención: Busca tener un control sobre los factores que pueden promover un fraude, especialmente de las actividades que desempeñan las personas que tienen acceso a una red, así como también controlar la información confidencial que puede afectar determinados bienes o servicios.

Detección: Referente al descubrimiento o identificación de forma oportuna y certera de un fraude anteriormente realizado.

Solución: Consiste en el conjunto de acciones y decisiones a tomar para eliminar o reducir al máximo el origen de un determinado tipo de fraude.

Disuasión: Tiene como objetivo principal persuadir o convencer a la comunidad en general de las consecuencias negativas que implica realizar un acto ilegal como es el fraude.

En la figura 2.2 se ilustra el proceso realizado para controlar el fraude.

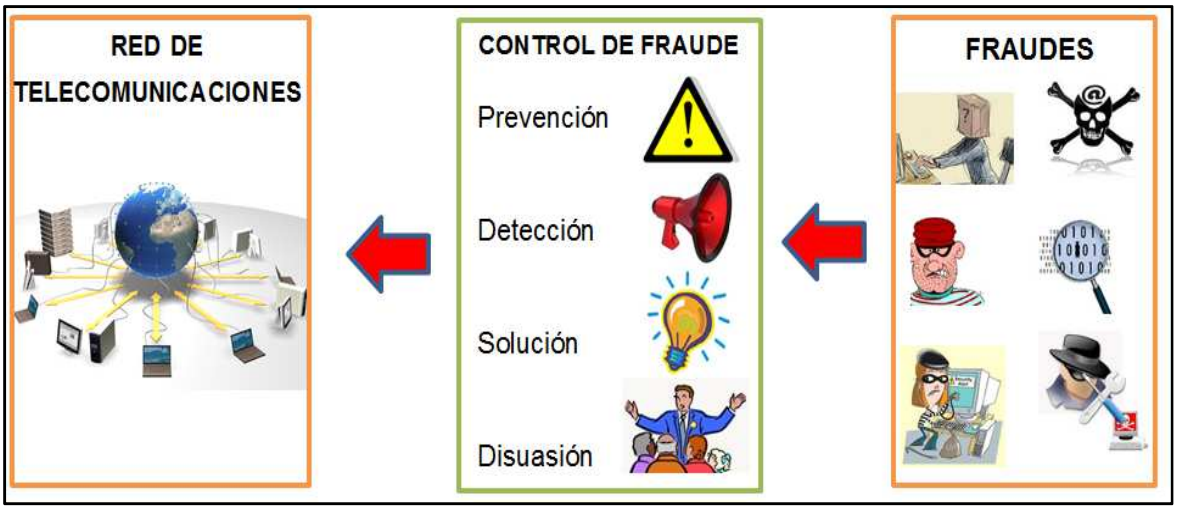

Figura 2.2 Proceso de control de fraude

2.5 DEPARTAMENTO DE PREVENCIÓN DE FRAUDE.

Para las empresas que brindan servicios de Telecomunicaciones es de suma importancia contar en su estructura organizacional con un departamento destinado a detectar y mitigar potenciales situaciones de fraude que pudieran generar perjuicios a las mismas, en base al monitoreo y control permanente sobre la gestión y servicios provistos, generando recomendaciones y verificando el cumplimiento de las mismas.

Las principales funciones que debe cumplir esta área son:

- Evaluar procedimientos y procesos de las diversas áreas de la empresadesde la perspectiva de prevención de fraude para generar recomendaciones de mejora y fortalecimiento del control.
- Administrar los sistemas de control de fraude que utilizan las empresas de telecomunicaciones, asegurando su permanente operación y eficacia.
- Realizar el seguimiento y control permanente del comportamiento de tráfico y servicios para detectar comportamientos atípicos y potenciales situaciones de fraude, a fin de determinar sus causas generando las respectivas acciones de corrección y control.
- Evaluar vulnerabilidades desde el punto de vista de fraude de los productos y servicios provistos por la empresa.

- Establecer estadísticas e indicadores que permitan evaluar la eficacia de los controles y gestión de prevención de fraude.
- Evaluar e informar respecto del nivel de cumplimiento de las acciones correctivas en eventos de fraude.
- Proporcionar soporte y apoyo a organismos técnicos de controly operadoras de servicios de telecomunicaciones desde la perspectiva de fraude en telecomunicaciones enmarcados en la normatividad vigente.

2.6 MARCO REGULATORIO PARA FRAUDES EN TELECOMUNICACIONES.

Actualmente rige en Ecuador una amplia base legal para poder combatir el fraude en Telecomunicaciones. En la Ley Especial de Telecomunicaciones publicada el 13 de marzo del 2000, el artículo 27 detalla sobre las sanciones correspondientes a delitos contra las telecomunicaciones lo siguiente: “Los delitos cometidos contra los medios y servicios de telecomunicaciones serán los tipificados en el Código Penal y serán sancionados de conformidad con lo dispuesto en dicho código”. [35]

En el código penal el artículo 422 menciona: “Quienes ofrezcan, presten o comercialicen servicios de telecomunicaciones, sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios o cualquier otra forma de contratación administrativa, salvo la utilización de servicios de internet, serán reprimidos con prisión de dos a cinco años.” [36]

2.7 TIPOS DE FRAUDES EN TELEFONÍA. [33][34][37]

2.7.1 FRAUDE POR SUSCRIPTOR. [33][37]

Este tipo de fraude consiste en la falsificación o alteración de documentos suplantando la identidad de terceras personas con el fin de que los cargos se registren a nombre de ellas. El defraudadorrealiza el máximo uso posible de la línea telefónica hasta que es suspendida por falta de pago afectando la imagen de las personas suplantadas, las cuales son registradas como usuarios morosos; aunque la empresa prestadora del servicio es quien se ve más afectada por no poder cobrar por el consumo realizado en la línea telefónica.

2.7.1.1 Detección y control.

Dentro de una empresa de Telecomunicaciones, es importante contar con un departamento que se encargue de la verificación de la veracidad de los datos del suscriptor previo a la firma del contrato de servicio. Se debe tener un proceso minucioso de validación de información del suscriptor para evitar el fraude por suscripción. En la figura 2.3 se indica el proceso de fraude por suscripción.

Figura 2.3 Fraude por suscripción [33]

2.7.2 FRAUDE CLIP-ON. [34][37]

Esta modalidad de fraude ocurre cuando el defraudador sustrae una línea telefónica activa desde la acometida de la red externa o desde el armario para llevarla hacia su domicilio y realizar llamadas cuyo consumo será cobrado al suscriptor de la línea.

El principal afectado por este tipo de fraude es el suscriptor de la línea telefónica puesto que debe pagar el consumo realizado por el infractor en el caso en que no se compruebe el fraude. Además la empresa prestadora del servicio se ve afectada en la imagen y en daños provocados en su infraestructura.

2.7.2.1 Detección y control.

Este tipo de fraude se lo detecta generalmente mediante reclamos realizados por los clientes dueños de líneas robadas, quienes se ven afectados en un incremento considerado de sus facturas. El fraude clip on también es detectado por los especialistas de fraude de las empresas, quienes analizan el tráfico telefónico con el objetivo de encontrar comportamientos atípicos que puedan reflejar un posible fraude por robo de líneas o clip on.

2.7.3 FRAUDE DETERCER PAÍS. [33][34]

Se lo denomina así porque interviene un tercer país, como defraudador, para la comunicación entre los otros dos países. En este tipo de fraude el defraudador utiliza varias líneas telefónicas para comunicar a dos usuarios de diferentes países mediante un conmutador o una llamada en conferencia. En este proceso, el defraudador en un país Z llama a un destino en un país X, el cual solicita comunicarse con un destino en un país Y, la persona en el país Z marca hacia el destino del país Yy los deja en comunicación. El defraudador realiza todas las llamadas posibles hasta que las líneas sean suspendidas por falta de pago afectando directamente a las empresas proveedoras del servicio.

En la figura 2.4 se ilustra el fraude de Tercer País.

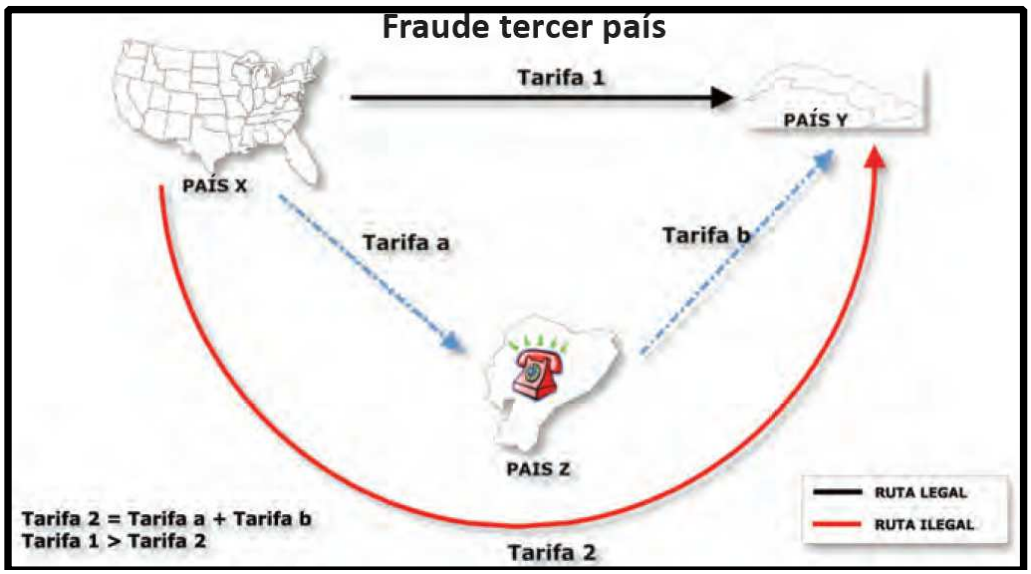

Figura 2.4 Fraude de Tercer País

2.7.3.1 Detección y control.

Se detecta por la presencia de llamadas hacia destinos internacionales atípicos. Cuando se identifica este tipo de llamadas el analista de fraude debe consultar la facturación de la línea que realiza la llamada así como también analizar el tráfico telefónico que presenta la misma con el fin de determinar un perfil de comportamiento.

2.7.4 FRAUDE DE PBX. [33][34][37]

Las Centrales Secundarias Privadas conocidas como PBX son usadas por las empresas para conectarse a la red telefónica pública conmutada. Estas centrales son vulnerables a sufrir ataques por parte de defraudadores que obtienen beneficios económicos al cobrar por llamadas de tráfico nacional, internacional, llamadas a teléfonos móviles entre otras; siendo perjudicadas las empresas dueñas de las PBX que tienen que pagar por las llamadas fraudulentas realizadas.

Este tipo de fraude es factible ya que las PBX cuentan con puertos de acceso remoto conocidos como DISA, estos puertos son usados para que empleados que se encuentran fuera de la empresa puedan realizar llamadas que son cargadas al número del PBX. Los defraudadores conocen las claves para poder acceder a la configuración de la PBX y poder lucrar mediante el uso ilícito de la misma.

En una PBX existe un puerto destinado al mantenimiento remoto, el defraudador logra acceder a este puerto mediante un módem y de esta forma realiza llamadas normalmente registradas en las noches y los fines de semana ocasionando un perjuicio económico directo a la empresa dueña de la PBX.En la figura 2.5 se indica un ejemplo de este tipo de fraude.

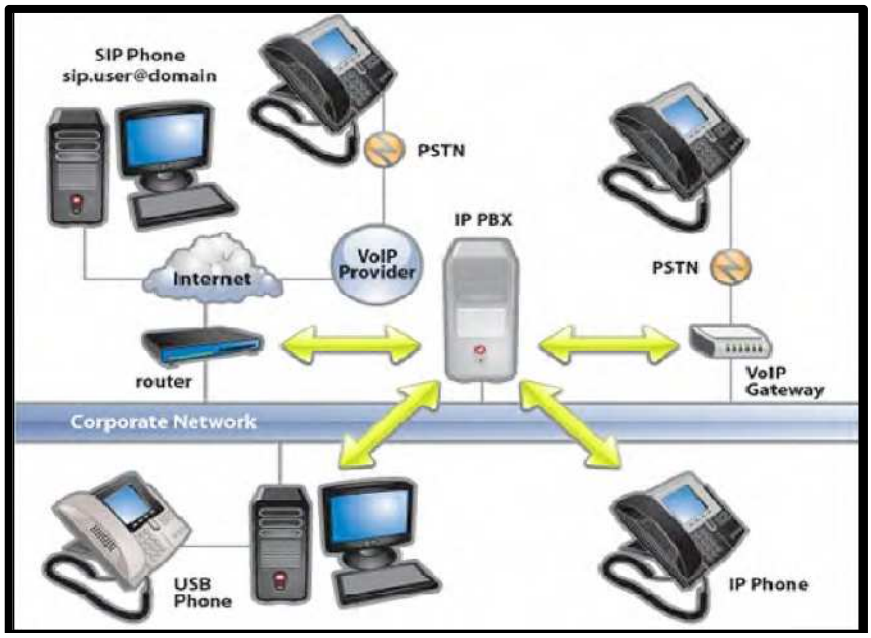

Figura 2.5 Fraude de PBX

2.7.4.1 Detección y control.

El principal responsable para evitar este tipo de fraude es la empresa propietaria de la PBX, la cual debe tener un control completo de las personas y de las claves de acceso para la configuración de su PBX. Cuando existe un incremento considerable de las llamadas realizadas desde la central de la empresa, es muy importante realizar un análisis de los destinos llamados así como también de los horarios de las llamadas realizadas para lograr detectar el origen de la actividad fraudulenta. Si la empresa no cuenta con personal especializado para la configuración de la PBX, es necesario contratar terceras empresas para garantizar el correcto funcionamiento y mantenimiento de la central privada de la empresa.

2.7.5 BY PASS [33][34][37]

Este tipo de fraude consiste en cursar tráfico internacional de un país A hacia un país B;impidiendo que el mismo pase por las centrales de tráfico internacional y de esta forma registrar en la tarificación una llamada internacional como llamada local.Los sistemas By-Pass son posibles ya que cuenta en su estructura con tres componentes: un enlace internacional, equipos que procesen la voz; y un lugar encubierto con un gran número de líneas telefónicas para llevar cada llamada

internacional a la central de una red local. En la figura 2.6 se ilustra un sistema Bypass con sus respectivos componentes.

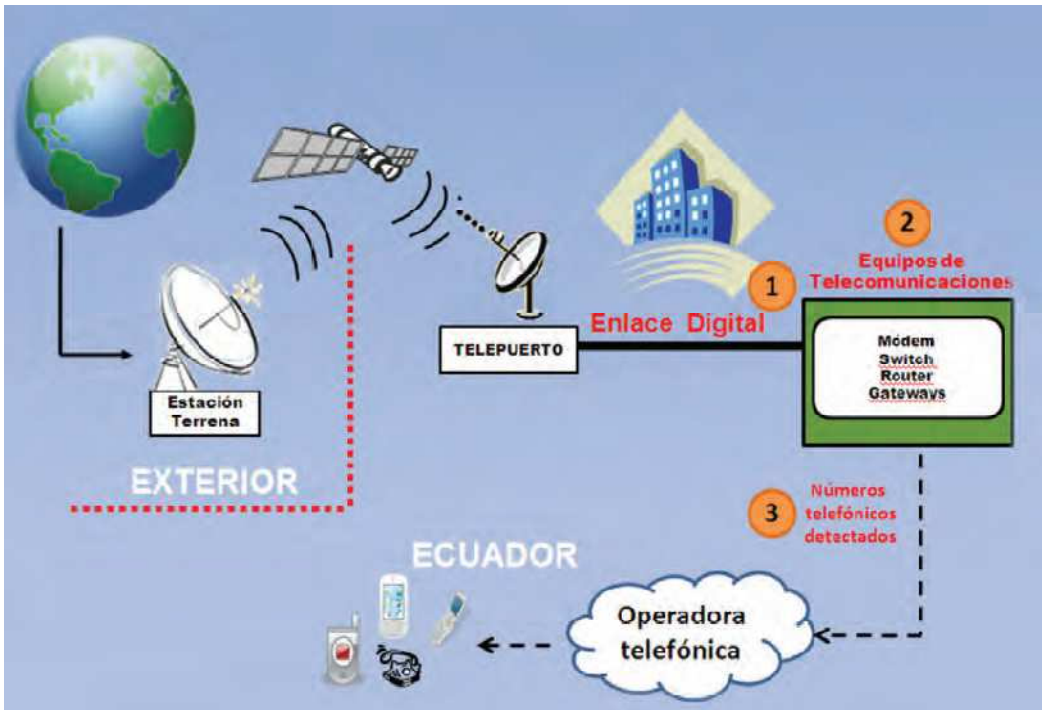

Figura 2.6 Componentes Sistema By – Pass [33]

Existen dos tipos de sistemas By Pass:

- **Entrante:** Es el tráfico internacional que ingresa desde otros países sin pasar por la central de tráfico internacional.
- **Saliente:** Es el tráfico internacional que sale de un país hacia el exterior. Se lo realiza generalmente mediante la venta de tarjetas de telefonía ilícitas, reventa de minutos, etc.

En la figura 2.7 se incluye imágenes de equipos de un sistema By Pass requisado por la Superintendencia de Telecomunicaciones.

Figura 2.7 Equipos de un Sistema By Pass requisado por la SUPERTEL [33]

A continuación se detallará el proceso como se realiza una llamada internacional legal y se la comparará con una llamada realizada mediante un sistema By Pass.

2.7.5.1 Ruta legal de una llamada internacional.

Este tipo de ruta se la ilustra en la figura 2.8.

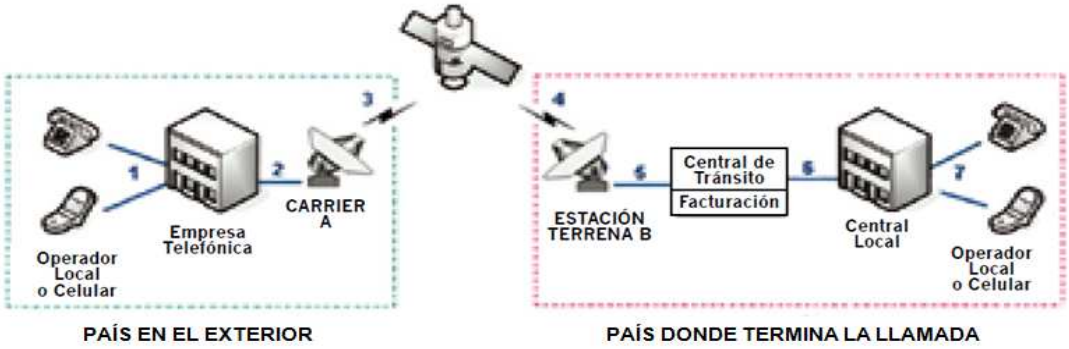

Figura 2.8 Ruta legal de una llamada internacional

En la tabla 2.1 se detalla el proceso legal de una llamada internacional.

Etapas	Descripción
1	El usuario en el país A marca el número del destino al que quiere llamar y esta llamada ingresa a la empresa telefónica local.
2	Llamada es transferida hacia el carrierA, establecido en el país origen.
3 y 4	Carrier A envía la llamada a la estación terrena B, establecida en el país destino.
5	La llamada es transportada a la central de tránsito la cual realiza la gestión de la llamada.
6	La llamada es transferida a la central local del país destino.
7	La central local enruta la llamada hacia el usuario final.

Tabla 2.1 Proceso legal de una llamada internacional.

2.7.5.2 Ruta ilegal de una llamada internacional.

Este tipo de ruta se la ilustra en la figura 2.9.

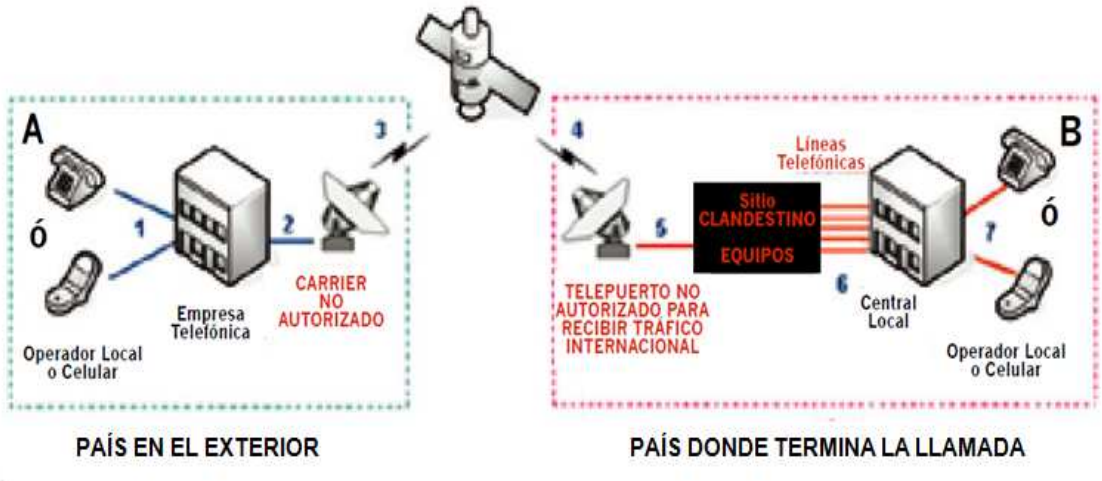

Figura 2.9 Ruta bypass de una llamada internacional

En la tabla 2.2 se detalla el proceso ilegal de una llamada internacional.

Etapas	Descripción
1	El usuario en el país A usa generalmente tarjetas de telefonía internacional para llamar hacia un destino en un país. Esta llamada se encapsula en paquetes IP e ingresa a la empresa telefónica local.
2	Se transfiere el paquete IP hacia el carrier no autorizado del país A.
3 y 4	Carrier A envía la llamada al telepuerto no autorizado en el país B.
5	Los paquetes IP son desencapsulados en el sitio clandestino.
6	Las llamadas son transferidas como locales hacia la central telefónica local mediante varias líneas telefónicas adquiridas ilegalmente por el defraudador.
7	La central local enruta la llamada hacia el usuario final.

Tabla 2.2 Proceso ilegal de una llamada internacional.

2.7.5.3 Detección y control.

Para poder detectar un sistema de fraude tipo By Pass, es necesario contar con un departamento especializado que se encargue de efectuar un procedimiento llamado pruebas de lazo. En este tipo de pruebas, se realiza llamadas (manualmente o automáticamente) desde el país en donde se quiere identificar el fraude, usando para ello tarjetas de telefonía internacional. El objetivo principal de las pruebas de lazo es obtener información acerca del carrier; si la llamada se la realizó legalmente el número identificado será un carrier legalmente establecido; caso contrario se identificará un número local, alarma de un posible sistema By Pass.

2.8 MÉTODOS DE CONTROL DE FRAUDE EN TELECOMUNICACIONES.

Actualmente los fraudes entelecomunicacionesperjudican económicamente a las empresas prestadoras de servicios limitando su capacidad de brindar más y mejores servicios a los usuarios o suscriptores. Es por ello que dichas empresas

están conscientes de la importancia de mejorar la detección y el combate del fraude en telecomunicaciones, ya que finalmente, al tener menos pérdidas ocasionadas por actos fraudulentos, se dispondrá de más recursos económicos que se puedan invertir en beneficio de la sociedad. Ahí radica la necesidad de contar con adecuados mecanismos de control que permitan una efectiva prevención, detección, análisis y disuasión de eventos de prestación de servicios de forma no legal que puedan generarse en la red de comunicaciones de una empresa.

Dentro de los principales métodos de control de fraude en telefonía se describe los siguientes:

2.8.1 LLAMADAS DE PRUEBA DE TRÁFICO TELEFÓNICO INTERNACIONAL.

Este tipo de método de control de fraude se basa en la realización de llamadas internacionales con el fin de encontrar irregularidades en éstas, que generen señales de alerta sobre la presencia de posibles actividades fraudulentas.El propósito de estas pruebas es monitorear los canales y rutas que se están utilizando para comunicarse con el país a través de una red de telefonía. Existen diferentes mecanismos de llamadas de prueba como son:

2.8.1.1 Pruebas de lazo telefónico internacional (loop). [34]

Su funcionamiento se basa en la generación manual o automática de llamadas internacionales desde el país donde se quiere identificar el fraude, usando para ello tarjetas de telefonía internacional. Todas estas llamadas se ejecutan hacia líneas terminales que son de propiedad de quien realiza la prueba, con el objetivo de obtener información acerca del número telefónico origen y real por el cual ingresó la llamada. Cuando una llamada internacional ingresa a través de una ruta normal, el teléfono de prueba identifica un número asignado al carrier internacional que procesó la llamada; sin embargo, cuando la llamada fue recibida a través de un sistema ilegal, el identificador de llamadas registra un número local, del cual posteriormente se obtiene la localización exacta y la información de la persona a la cual pertenece la línea telefónica. En la figura 2.10 se ilustra una prueba de lazo telefónico internacional.

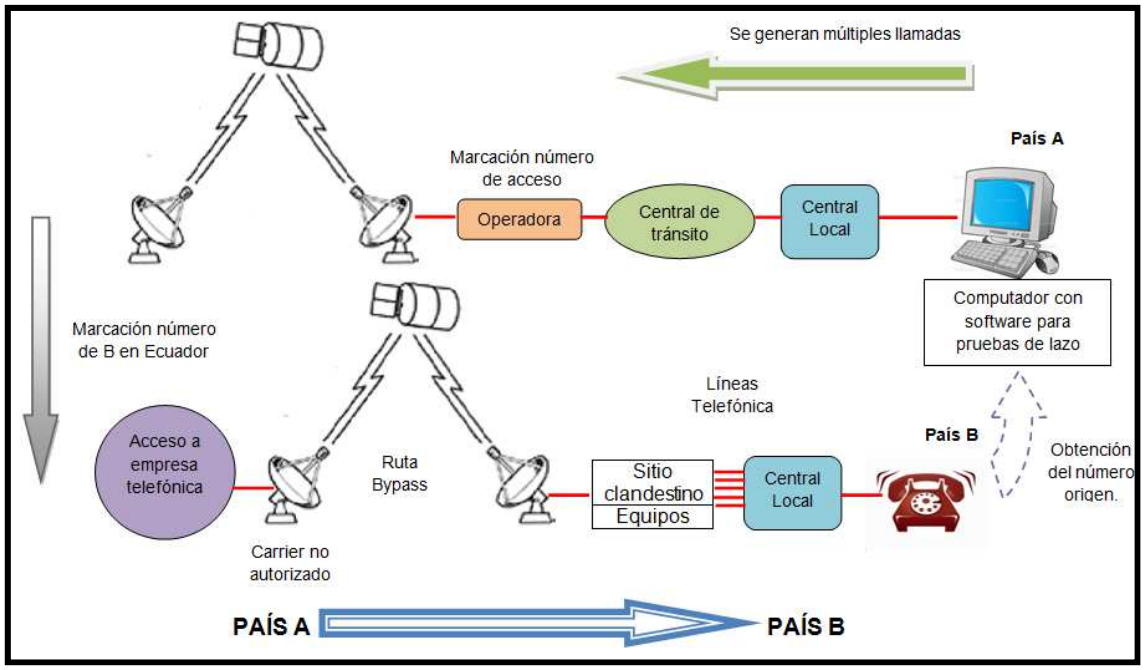

Figura 2.10 Prueba de lazo telefónico internacional. [34]

El principal objetivo de este método de control es el de detectar en forma técnica los números de las líneas telefónicas que presuntamente están siendo utilizadas para cursar de manera no autorizada llamadas de origen internacional hacia las redes de operadoras telefónicas autorizadas en un determinado país. Permite detectar líneas que estén cursando tráfico telefónico internacional entrante no autorizado a través de operadores de Voz sobre IP (VoIP) y tarjetas de telefonía internacional prepagadas.

2.8.1.2 Bombardeo de llamadas.

Consiste en realizar llamadas desde distintos países a varios números telefónicos previamente seleccionados pertenecientes a una red de telecomunicaciones con el objetivo de detectar líneas que cursen tráfico telefónico internacional entrante no autorizado. Es decir que verifica el correcto ingreso de llamadas internacionales entrantes desde redes de telefonía hacia la red de le empresa de telecomunicaciones que realiza el control a través de rutas tipo “carrier” autorizados. Este tipo de mecanismo se indica en la figura 2.11.

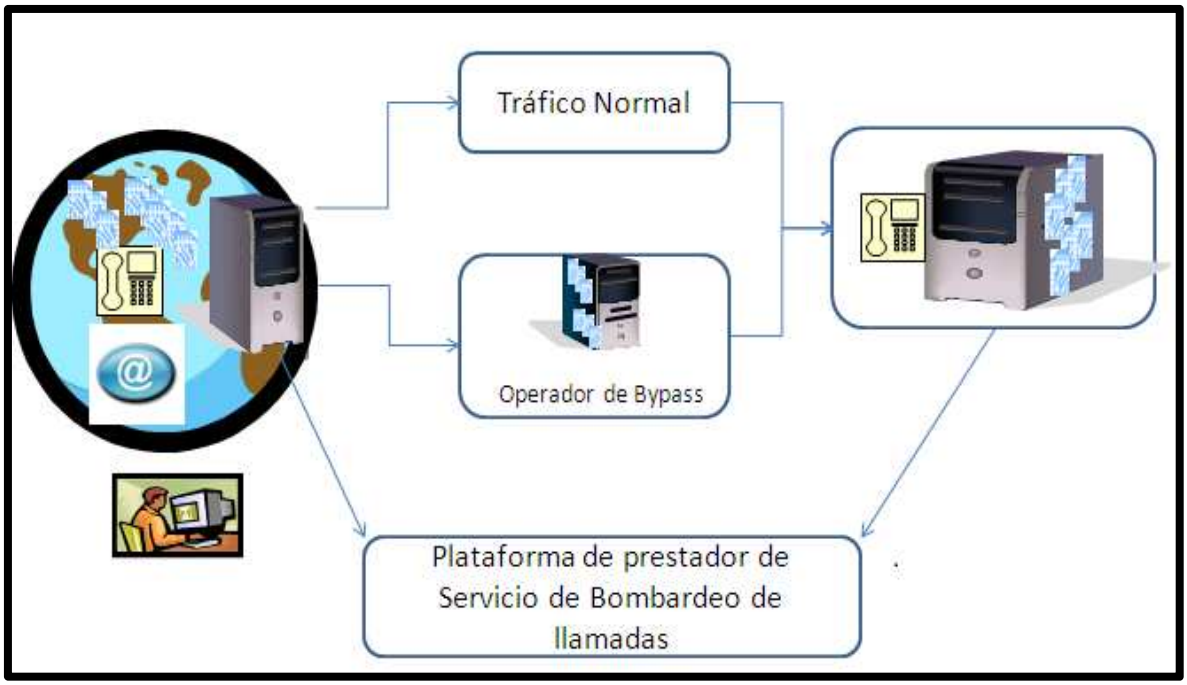

Figura 2.11 Bombardeo de llamadas

2.8.2 PERFILAMIENTO DE TRÁFICO TELEFÓNICO. [37]

Este tipo de método analiza el tráfico cursado por las líneas telefónicas que conforman una red con el fin de identificar aquellas que presentan un comportamiento atípico, indicador de un potencial escenario de fraude.Este método implica la determinación y cuantificación de parámetros que alertan el uso de una línea telefónica en actividades irregulares de telecomunicaciones. El establecimiento de valores umbrales de dichos parámetros que integran una llamada telefónica constituyen verdaderos filtros que permiten identificar aquellos números telefónicos que están siendo utilizados en una presunta práctica ilícita de telecomunicaciones.

En la figura 2.12, se detalla los pasospara establecer un control de fraude mediante perfilamiento del tráfico telefónico.

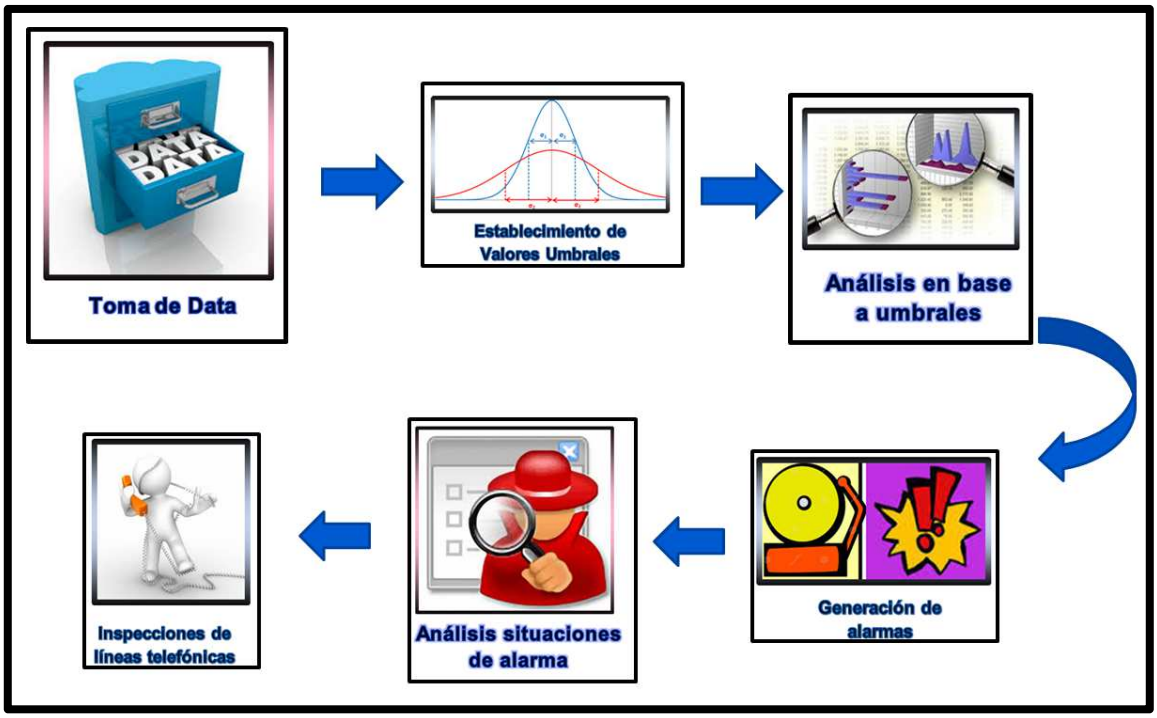

Figura 2.12 Perfilamiento de tráfico telefónico

El método de perfilamiento de tráfico telefónico se basa en analizar la información de una llamada creando perfiles de comportamiento de las líneas de telefonía y estableciendo valores máximos de ciertos parámetros de esta información dentro de los cuales se puede considerar que se presenta un comportamiento regular. Este tipo de control se basa en un método llamado análisis de CDRs que se explicará a continuación.

2.8.2.1 Análisis de CDRs.

Los CDRs son registros que contienen información muy importante sobre una llamada telefónica como el número de origen, número de destino, duración de llamada, número de llamadas entre otros. Todos estos parámetros son analizados para determinar el comportamiento que tiene cada una de las llamadas que generan una señal de alerta con el fin de garantizar que no existan actividades fraudulentas.

Cada uno de los campos que conforman un CDR es analizado en función de detectar diferentes tipos de fraude. Por ejemplo cuando un número de origen realiza muchas llamadas con destinos internacionales y recibe pocas llamadas, se presenta una alarma de que ese número llamante este siendo parte de un sistema

By Pass. Cuando un número realiza llamadas con un destino atípico, se presume la existencia de un fraude de tercer país,

En la figura 2.13 se muestran los principales campos de los CDRs y se relaciona a cada uno de ellos con los diferentes tipos de fraude que se pueden identificar mediante su análisis.

Número de origen	Número de destino	Hora de inicio de llamada	Hora de Fin de llamada	Duración de llamada	Fecha de inicio de llamada	Fecha de fin de llamada
022852XXX	0013219457XXX	23:45	04:45	300	01/06/2014	02/06/2014

Figura 2.13 Campos de CDR.

- **FraudeClipOn:** Este tipo de fraude se lo identifica estableciendo valores umbrales para los parámetros de los campos: número de destino, hora de inicio de llamada, hora de fin de llamada y duración de llamada. Además es muy importante determinar el número de llamadas que se ha realizado desde la línea. Valores inusuales en estos campos indican la posible presencia de fraude.
- **Fraude Tercer País:** Para lograr identificar Fraude de Tercer País, es necesario evaluar el campo de destino de llamadas acompañado con el número de llamadas realizadas. Varias llamadas a destinos atípicos dan la alerta de la existencia de este tipo de fraude. También se analiza el campo de duración de llamada.
- **Fraude de PBX:** En una empresa que cuenta con una PBX, es común que sufra fraude por llamadas de terceros. Este tipo de fraude se puede identificar analizando principalmente los campos: número de destino, hora de inicio llamada, hora de fin de llamada y fecha de inicio y fin de llamada. Llamadas hechas en horarios fuera de oficina, en horas inusuales y a destinos internacionales o celulares, indican la sospecha de actividad fraudulenta.
- **Bypass:** Este tipo de fraude se lo detecta en forma similar al de refilling. Se debe analizar dentro de los CDRs los campos de origen de llamada, destino de llamada y duración con el fin de determinar el comportamiento de las líneas telefónicas. Cabe mencionar que resulta muy complejo identificar este tipo de fraude con el método de análisis de CDRs, por lo

cual se cuenta con el método de pruebas de lazo telefónico internacional descrito anteriormente.

En la tabla 2.3 se resume los campos de los CDRs que se evalúan para cada uno de los fraudes analizados.

	Número de origen	**Número de destino**	**Hora de inicio de llamada**	**Hora de Fin de llamada**	**Duración de llamada**	**Fecha de inicio de llamada**	**Fecha de fin de llamada**
Clip On	X	X	X	X	X	X	X
Tercer País	X	X			X		
PBX	X	X	X	X	X		
Bypass	X	X			X		

Tabla 2.3 Campos de CDRs evaluados en cada fraude

CAPÍTULO 3.

ANÁLISIS DE LOS PROTOCOLOS DE SEÑALIZACIÓN DENTRO DE LA RED DE SERVICIOS TELEFÓNICOS DE CNT MEDIANTE EL USO DE SONDAS DE SEÑALIZACIÓN.

Para poder analizar los protocolos de señalización que intervienen en el establecimiento y gestión de una llamada telefónica, las empresas de telecomunicaciones usan equipos denominadosanalizadoreso sondas de protocolos. El monitoreo de una red tiene varios propósitos como son:análisis de las prestaciones de una red, control de la calidad del servicio, detección de fraudes, facturación entre otros.

En el caso del presente proyecto, se utilizó una sonda de señalización perteneciente a la Corporación Nacional de Telecomunicaciones, para monitorear el tráfico telefónico con el objetivo de detectar posibles escenarios de fraude en el servicio de telefonía que proporciona dicha empresa.

3.1 DESCRIPCIÓN DEL EQUIPO. [38]

El equipo que se utilizó fue una sonda de señalización PANTERA 100, fabricada por Sistemas Accanto. Dicha sonda es capaz de analizar el tráfico en base a filtros definidos y que pueden extraer datos de interés específico.

Esta sonda permite extraer información integral acerca de una llamada telefónica, es decir que proporciona datos sobre campos específicos de los CDRs en base al análisis de protocolos de señalización empleados en telefonía. Estos datos son recopilados en archivos de texto plano, los cuales se los puede exportar hacia una base de datos para su respectivo procesamiento.

3.1.1 CARACTERÍSTICAS GENERALES. [38]

En la tabla 3.1 se describen las principales características de la sonda de señalización PANTERA 100.

Sistema Operativo	Microsoft Windows XP Professional Real Time Operating System RTX
Software	Accanto Systems basic Operating System SW
Almacenamiento	80 GBytes.
Procesador	Intel QuadCoreXeon X3220. 2.4 GHz
Puertos USB	4 puertos USB 2.0
NIC	2 de 10/100/1000 Mbps para redes LAN cliente servidor.

Tabla 3.1 Características Generales PANTERA 100.

3.1.2 INTERFACES DE MEDICIÓN SOPORTADAS. [38]

E1: PANTERA 100 dispone de 4 puertos E1 para monitoreo y simulación.

Ethernet LAN: Este equipo puede realizar pruebas de medición para velocidades de 10 y 100 Mbps así como también de 1 y 10 Gbps. Para ello dispone de 4 puertos.

STM-1:PANTERA 100 dispone de4 puertos para monitoreo en ATM, estos puertos son utilizados en fibra óptica.

3.1.3 COMPONENTES FÍSICAS DE PANTERA 100. [38]

Para el buen uso del equipo es muy importante reconocer sus diferentes componentes física con el objetivo de optimizar el uso de PANTERA 100; las mismas que se muestra en la figura 3.1

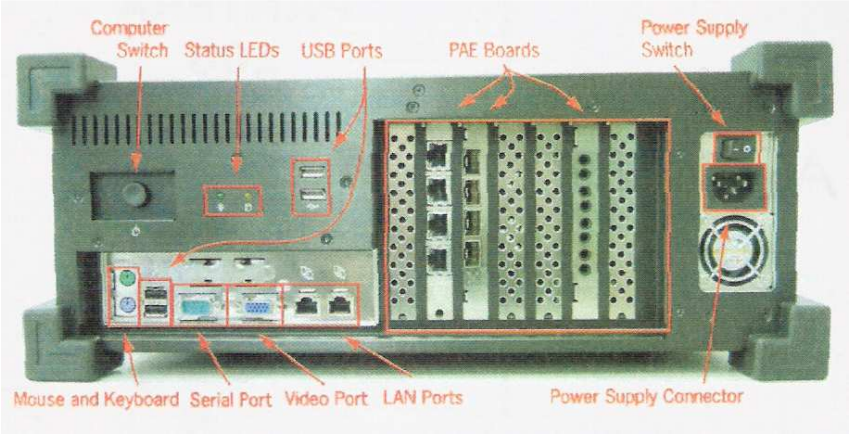

Figura 3.1 Componentes Físicas de Pantera 100. [38]

3.1.4 PROTOCOLOS SOPORTADOS.[38]

PANTERA 100 es un equipo que puede analizar una extensa variedad de protocolos entre los cuales se destacan los detallados en la tabla 3.2.

TELEFONÍA MÓVIL	**GSM**	SMS, SMPP
		SS7 ISUP
		INAP
		H.248/GCP
		SS7 para Banda Ancha.
	CDMA 2000	SS7 ISUP
		AIN
		SS7 para Banda Ancha
	UMTS	Release 99
		3GPP NBAP
		Gn/Gp/Ga (GTP)
TELEFONÍA FIJA	**SIGTRAN**	SCTP
		M2UA
		M2PA
		M3UA
		SUA
		IUA
	VoIP	H.323
		SIP
		MGCP
		RTP/RTPC
		MEGACO/H.248

Tabla 3.2 Protocolos soportados por PANTERA 100.

3.2 CONFIGURACIÓN PARA PRUEBAS DE MONITOREO. [38]

Para poder realizar las pruebas respectivas con la sonda de señalización PANTERA 100, se debe seguir el siguiente procedimiento.

a) Configuración de una prueba.

Dentro de la pestaña *File*, se selecciona la opción *New* para poder realizar una nueva prueba y se despliega una ventana como la que se muestra en la figura 3.2

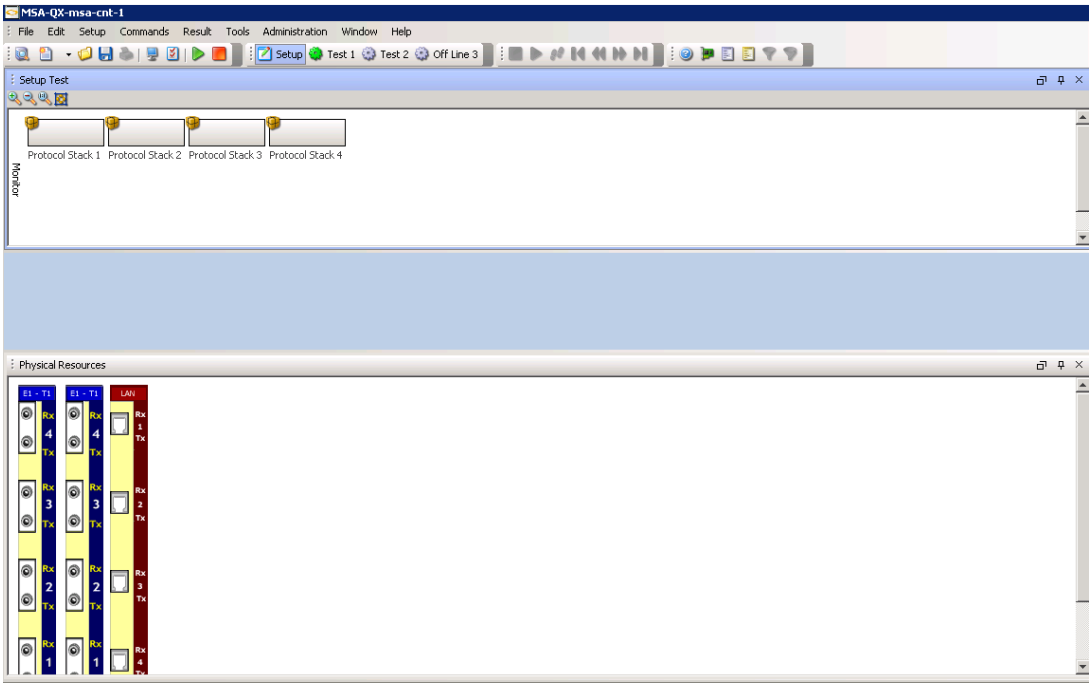

Figura 3.2 Ventana de Interfaces Físicas Pantera 100

En la figura 3.2 se puede observar que existen 2 regiones: la región que permite configurar los diferentes aspectos de cada una de las interfaces y la región de recursos físicos, la cual es una representación de lo que se tiene físicamente en el equipo.

b) Configuración de la capa física.

Como se indicó anteriormente, existen diferentes interfaces que se pueden sondear con PANTERA 100 como son: Ethernet, E1 Y STM-1. En este proyecto se sondearán protocolos basados en IP, configurando para ello la capa física Ethernet.Hay algunos aspectos importantes a ser tomados en cuenta como el modo de transferenciahalf o full dúplex, velocidad, aspectos de seguridad, etc.

La manera más conveniente para realizar pruebas en la capa física Ethernet, es monitorear todos los paquetes LAN deseados de la red configurando un puerto en el switch como puerto mirror o puerto de monitoreo.

Dentro de la región de recursos físicos se escoge el puerto Ethernet que se utilizará para monitorear la red y se lo ubica en la parte de configuración de prueba, donde se puedeescoger manualmente la velocidad.

En la figura 3.3 se ilustra la ventana de Configuración de las interfaces físicas de Pantera 100.

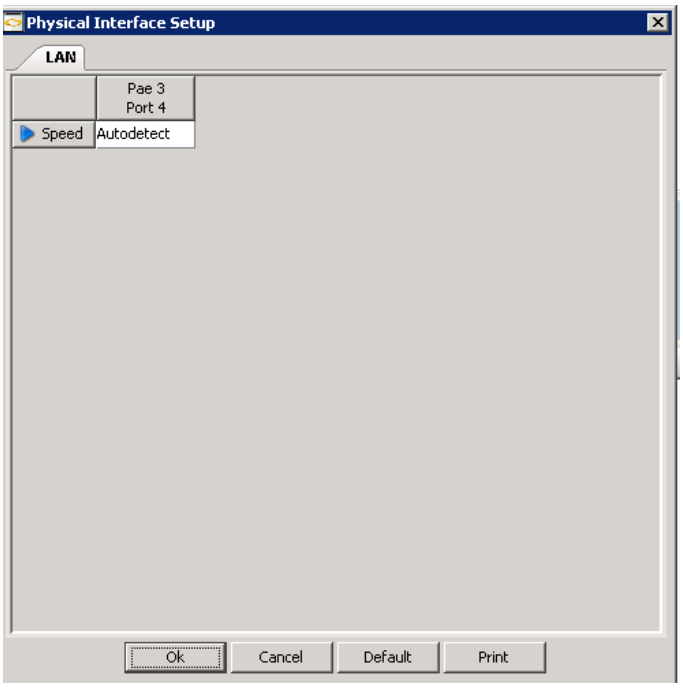

Figura 3.3 Configuración de las interfaces físicas de Pantera 100

c) Configuración de las opciones de una prueba.

Dentro de una prueba se puede configurar varias opciones como son:

Opciones de grabado de archivos. [38]

Nombre del archivo: Permite establecer un nombre para los archivos que se van a generar.

Descripción: Permite agregar una breve descripción sobre el archivo que se generará.

Tamaño del archivo: Máxima cantidad de memoria que se va a usar para grabar la prueba.

Avanzado: Permite al usuario decidir si se graban o no los trazos, CDRs, alarmas, estadísticas por separado y el tamaño máximo que tendrán dichos archivos.

Número de archivos: Configura el número de archivos que el sistema creará. Una vez que el instrumento ha grabado dicho número de archivos, si se necesita grabar más datos, se sobrescribirá el archivo más antiguo.

Máximo tiempo de grabación permitido: Tiempo máximo definido en minutos después del cual se generará un nuevo archivo.

En la figura 3.4, se puede observar todos los campos que se describieron anteriormente.

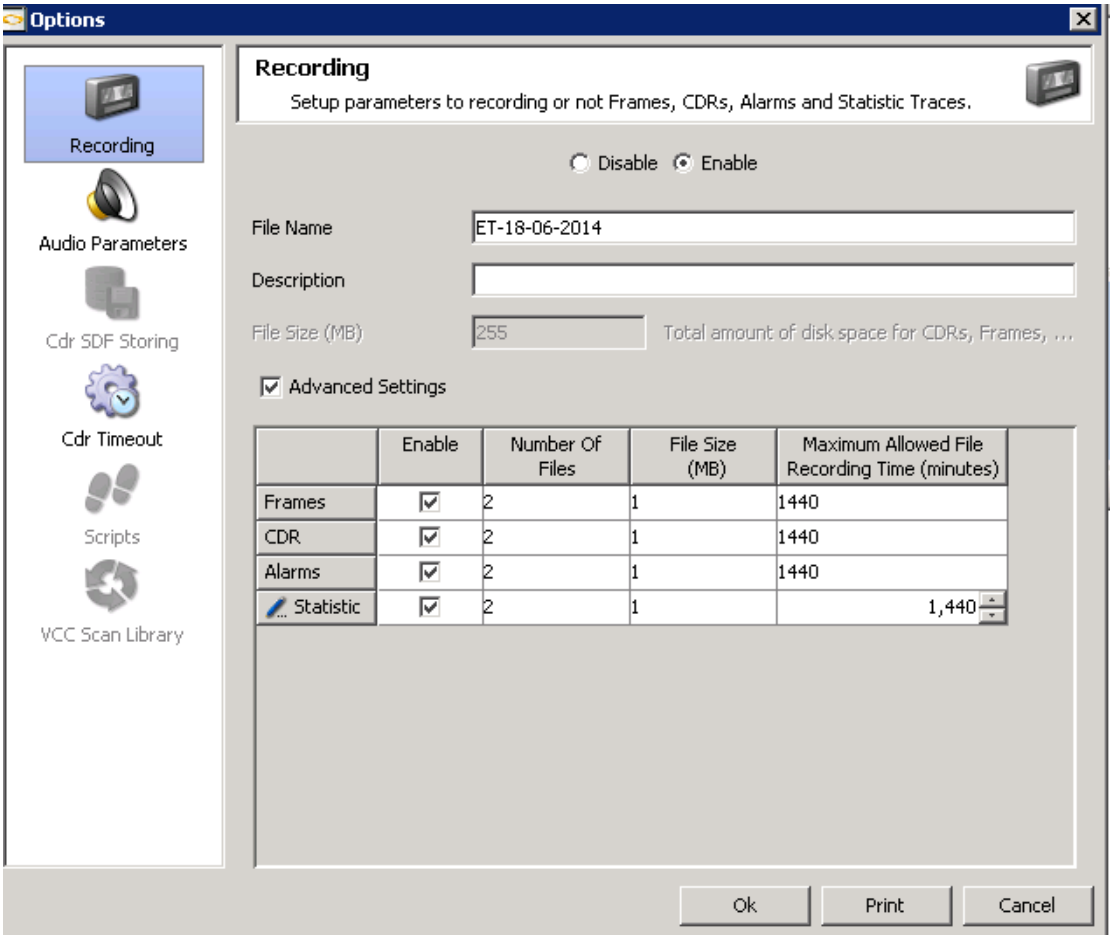

Figura 3.4 Opciones de grabado de archivos

Opciones de almacenamiento de CDRs en formato SDF.

Esta opción habilita la posibilidad de generar archivos SDF (formato de valores separados por coma).

La aplicación del cliente será responsable de transferir los archivos por medio de FTP y borrar los archivos del disco duro.

Una de las opciones de almacenamientoexistentes la llamada campos entrantes, la cual especifica el número de campos del CDR que serán grabados en el SDF. Si el usuario requiere por ejemplo los primeros 40 campos de un CDR, se ingresa dentro de esta opción el valor de 40.

En la figura 3.5 se indica la ventana en la cual se puede configurar las opciones de grabado de archivos en formato SDF.

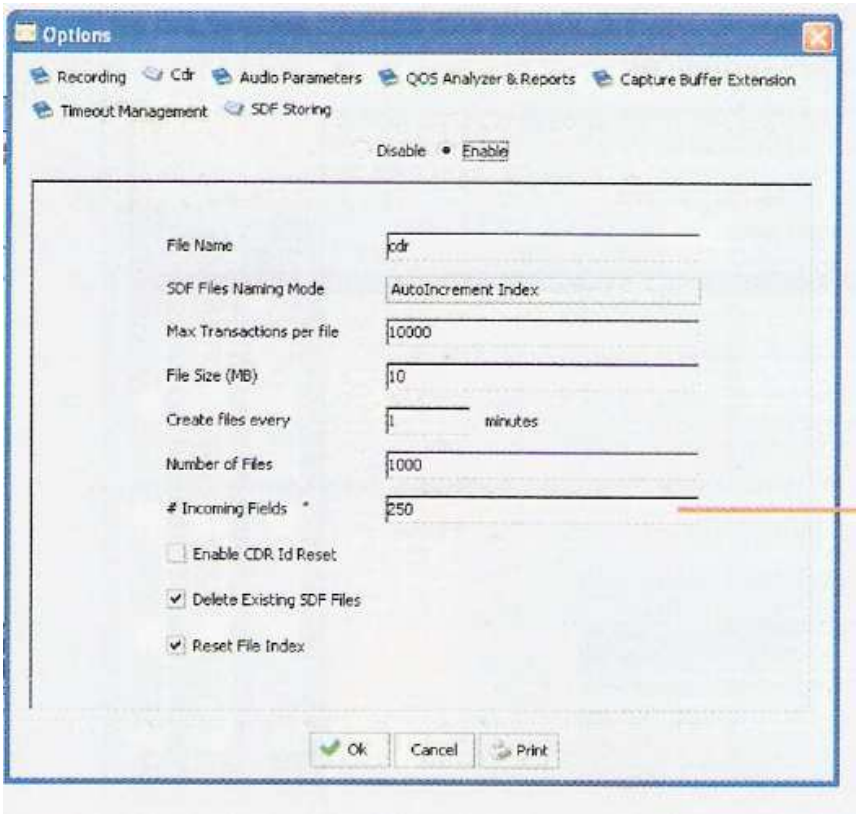

Figura 3.5 Opciones de grabados de archivos en SDF

d) Configuración del filtrado de resultados.

Cada característica de un protocolo puede ser configurado como un diferente filtro. Estos tipos de filtro están basados en operadores lógicos OR y AND.

En la figura 3.6 se observa la ventana en la cual se puede configurar las opciones de filtrado de resultados.

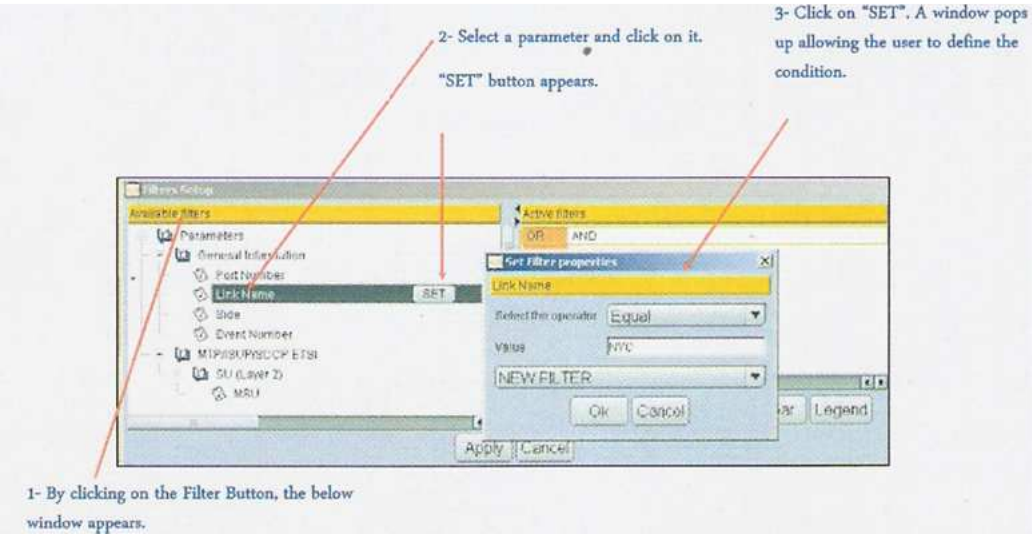

Figura 3.6 Configuración de filtrado de resultados. [38]

e) Ejecución de la prueba.

Una vez configurados todos los parámetros anteriormente descritos, se ejecuta la prueba de monitoreo; para ello se selecciona el ícono de Ejecutar para poder obtener la información de los archivos que se extraerán de la sonda de señalización. En la figura 3.7 se indica la ventana en la cual se puede ejecutar la prueba de monitoreo.

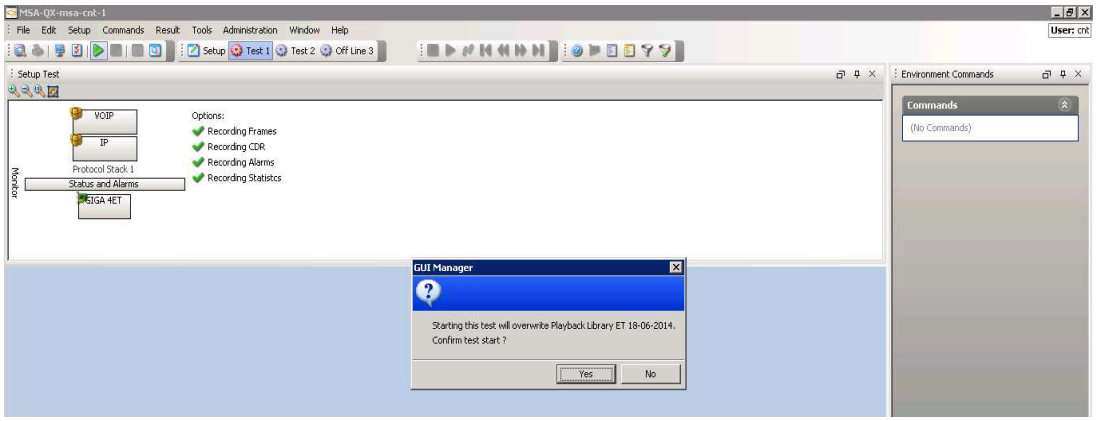

Figura 3.7 Ejecución de la prueba de monitoreo

3.3 OBTENCIÓN DE LOS RESULTADOS.

Posterior a la configuración y ejecución de las pruebas de monitoreo, PANTERA 100 genera los resultados de estas pruebas en archivos de texto plano. Todos los

archivos que se crean, se guardan en una carpeta predeterminada desde la cual se extraerá la información para importarla a una base de datos.

En los archivos de texto plano, los campos están delimitados por comas. La Figura 3.8 representa un ejemplo de un archivo de texto generado por la sonda de señalización.

```
1,PT_2010101367,1,78,,1,26,049438298,7112,27-JUN-2014 10:29:32.099 AM -05:00,27-JUN-2014 10:29:32.584 AM -
05:00,5,,,0,17,,0,0,7c92e95b360fd2ec7320bd7b05b7f2e9@10.208.42.18,1,0,0,10.208.42.18,10.208.26.20,,,sip:23956180@10.208.42.18
,,,,,,0,,10.208.42.18:10066,,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,1,,10.208.26.20,"7112"
<sip:23956180@10.208.42.18>,<sip:049438298@10.208.26.20>,,,,,,,,,,,Q.850,1,,Asterisk PBX
1.6.0.3,,,,,,,,,,,3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,,,,,,,,,,,,,1797840808,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,27-JUN-2014 10:29:32.099 AM -05:00,4,,,0,5750304653718992,5750304655707039,
```

Figura 3.8 Ejemplo de un archivo de texto plano

3.4 ANÁLISIS TEÓRICO DE LOS PROTOCOLOS DE SEÑALIZACIÓN PARA LA OBTENCIÓN DE CDRs.

Para realizar el análisis de los protocolos de señalización en función de obtener los campos de los CDRsdetallados en el capítulo 2, realizamos el siguiente procedimiento:

a) Sondeo de protocolos de señalización en los canales de comunicación utilizando el equipo PANTERA 100.

b) Análisis teórico de los datos obtenidos al sondear los protocolos de señalización para la obtención de los CDRs.

c) Procesamiento de los CDRs obtenidos del análisis previo de los protocolos.

A continuación se explica mediante ejemplos el proceso realizado para obtener los campos de los CDRs de las llamadas telefónicas mediante el análisis teórico de los protocolos de señalización SIP y SIGTRAN.

3.4.1 PROTOCOLOS SIGTRAN

Para fines explicativos, se tomó como ejemplo una llamada telefónica, mediante señalización SIGTRAN, que fue sondeada con el equipo PANTERA 100

obteniendo de la misma los siguientes datos que conforman el CDR. Estos datos son los que nos proporciona finalmente la sonda de señalización.

Número de Origen: 22378XXX.

Número de Destino: 22658XXX.

Duración: 64.9 segundos

Fecha de Inicio: 21 de septiembre del 2014.

Fecha de fin: 21 de septiembre del 2014.

Hora de inicio: 06:16:49.911 PM

Hora de Fin: 06:17:54.831 PM.

Número de Origen y Destino:

Al igual que cualquier paquete de datos, una llamada telefónica basada en VoIP debe seguir una determinada ruta cumpliendo con un proceso establecido. Existen tres capas dentro de este proceso como se indica en la figura 3.9.

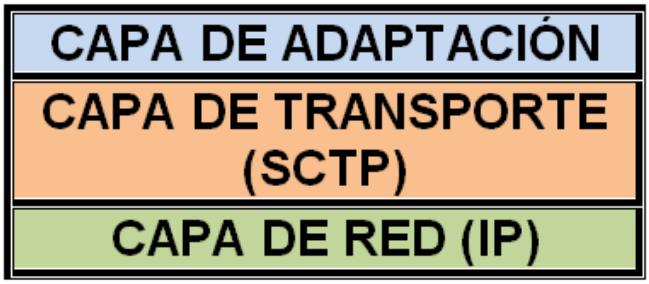

Figura 3.9 Capas de Arquitectura SIGTRAN.

Capa de adaptación:

Son capas de adaptación que soportan primitivas específicas para cada protocolo de la pila SS7 que se necesite transportar. En esta capa un solo protocolo puede ser implementado a la vez. En la red de telefonía de la Corporación Nacional de Telecomunicaciones se usa el protocolo M2UA para telefonía fija.

En el capítulo uno, se detalló la trama para el protocolo M2UA. A continuación se procederá a realizar el análisis de cada uno de los campos de esta trama para la llamada telefónica en ejemplo.

Para la cabecera común se obtuvo los siguientes datos ilustrados en la figura 3.10.

VERSIÓN: 1.0								RESERVA								CLASE DE MENSAJE: M2UA								TIPO DE MENSAJE: Datos							
Valor: 01								Valor: 00								Valor: 06								Valor: 01							
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1
LONGITUD DE MENSAJE																															
Valor: 32																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0

Figura 3.10 Datos de llamada telefónica en cabecera común M2UA

Además se encontró un parámetro de longitud variable con la información que se indica en la figura 3.11.

ETIQUETA DEL PARÁMETRO: Interface Id. (Integer type)																LONGITUD DEL PARÁMETRO: 8															
Valor: 01																Valor 8															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	
VALOR DEL PARÁMETRO: 7																															
Valor : 07																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	

Figura 3.11 Datos de llamada telefónica en parámetro de longitud variable M2UA

Capa Transporte:

Dentro de esta capa se encuentra el protocolo SCTP, el cual es un protocolo de transporte IP y trabaja al mismo nivel que los protocolos TCP y UDP de la capa de transporte de la arquitectura TCP/IP.

SCTP se usa para transporta los mensajes de SS7 fiablemente sobre las redes IP. Es un protocolo orientado a conexión; es decir que uno de los terminales proporciona al otro una lista de sus direcciones de transporte (múltiples direcciones IP en combinación con un puerto SCTP). Está diseñado parar soportar el envío de mensajes de señalización sensibles al tiempo.

En el capítulo uno, se detalló la trama para el protocolo SCTP. A continuación se procederá a realizar el análisis de cada uno de los campos de esta trama para la llamada telefónica en ejemplo.

En la figura 3.12 se puede observar los datos obtenidos en una trama SCTP de una llamada telefónica.

PUERTO DE ORIGEN: 2922																PUERTO DESTINO: 2922															
Valor: 0B																Valor: 0B															
0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1
VERIFICACIÓN DE ETIQUETA: 3595703794																															
Valor: 214																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0
CHECKSUM : 1956987762																															
Valor: 74																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0
TIPO DE CHUNK: SACK (Selective Acknowledge)								BANDERA DE CHUNK:								LONGITUD DE CHUNK: 16															
Valor: 03								Valor: 00								Valor: 16															
0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
DATOS DE INFORMACIÓN DEL CHUNK																															

Figura 3.12 Datos de llamada telefónica en la trama SCTP.

Capa Red.

Esta capa está a nivel de la capa de red de la arquitectura TCP/IP. Su función es la de proporcionar los servicios de envío, enrutamiento y control de congestionamiento de los paquetes de datos de un nodo a otro en la red formando una interfaz entre los abonados y la red de telefonía presentando un esquema de direccionamiento para direcciones de la red. Dentro de este

esquema de direccionamiento se asigna además, mediante una configuración de la empresa prestadora de servicio, los diferentes números telefónicos a las direcciones IP.

En la figura 3.13 se observael paquete IP dentro del proceso de una llamada telefónica mediante señalización SIGTRAN.

VERSIÓN: IPV4				Tamaño de Cabecera				TIPO DE SERVICIO								LONGITUD TOTAL: 96															
Valor: 4				Valor: 5												Valor: 96															
0	1	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
								P				D	T	R	Rsv																
IDENTIFICACIÓN: 5927																BANDERAS DE FRAGMENTO			POSICIÓN DEL FRAGMENTO												
Valor: 17																			Valor: 0												
0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
																Rsv	D F	M F													
TIEMPO DE VIDA								PROTOCOLO: SCTP								COMPROBACIÓN DE CABECERA: 60774															
Valor: 253								Valor: 84								Valor: 237															
1	1	1	1	1	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1
DIRECCIÓN IP ORIGEN: 200.107.63.2																															
Valor: 200																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0
DIRECCIÓN IP DESTINO: 172.23.5.7																															
Valor:172																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	0	0

Figura 3.13Datos de llamada telefónica en datagrama IP

Una vez extraídas las direcciones de red de origen y destino, se puede asignar a las mismas sus respectivos números telefónicos y de ésta forma obtener estos dos campos muy importantes de los CDRs.

Duración de llamada.

Para obtener la duración de la llamada, se debe tener información de los intervalos de tiempo en los que se efectuó cada uno de los pasos que conforman el establecimiento y gestión de una llamada telefónica. Para el ejemplo se obtuvo los siguientes datos con respecto a los tiempos como indica la figura 3.14.

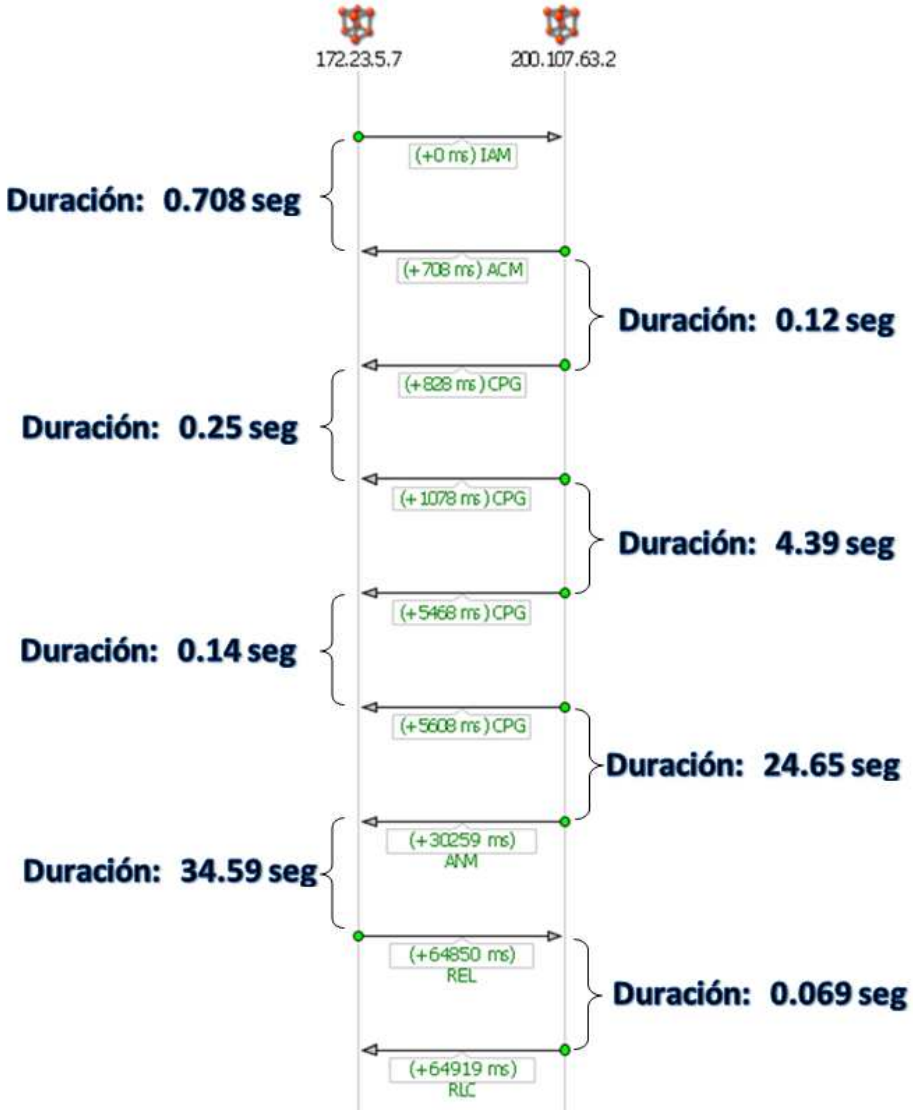

Figura 3.14 Establecimiento de una llamada telefónica mediante SIGTRAN.

En la tabla 3.3 se detalla las transferencias de cada uno de estos mensajescon el objetivo de tener una idea más clara de los tiempos de la gestión y establecimiento de la llamada telefónica de ejemplo.

Proceso	Descripción	Duración (segundos)
IAM	Mensaje de Dirección Inicial mensaje. Contiene el número origen y destino.	0.708
ACM	Mensaje de Dirección Completa. Mensaje generado por el destino cuando la llamada comienza.	0.12

Tabla 3.3 Tiempos de duración de una llamada mediante SIGTRAN

Proceso	Descripción	Duración (segundos)
CPG	Llamada en progreso. Tiempo adicional de gestión de llamada.	29.43
ANM	Mensaje de Respuesta. Generado cuando la llamada fue contestada	34.59
REL	Pedido de liberación de llamada	0.069
RLC	Liberación de llamada completada.	Fin de llamada. Se produce de forma instantánea.
Tiempo total de gestión de llamada		**30.32**
Tiempo total propiamente de llamada		**34.59**
Duración Total.		**64.91**

(Continuación)Tabla 3.3 Tiempos de duración de una llamada mediante SIGTRAN

Campos de Hora/Fecha de Inicio/Fin de llamada.

PANTERA 100, es un equipo destinado a sondear señalización en tiempo real; es decir que los datos obtenidos para hora y fecha de inicio y fin de llamada son capturados el momento justo en el cual se estableció la llamada telefónica, obteniendo de esta forma los campos mencionados del CDR.

3.4.2 PROTOCOLO SIP.

A continuación se indica la forma de obtener los datos de los campos de los CDRS en una llamada telefónica mediante señalización SIP, que fue sondeada con el equipo PANTERA 100, obteniendo de la misma los siguientes datos que conforman el CDR extraído con la sonda de señalización.

Número de Origen: 46044XXX

Número de Destino: 22829XXX

Duración: 266.2 segundos

Fecha de Inicio: 3 de junio del 2014.

Fecha de fin: 3 de junio del 2014.

Hora de inicio: 11:48:22.784 AM.

Hora de Fin: 11:52:49.028 AM.

Número de Origen y Destino:

Como se indicó en el primer capítulo, el protocolo SIP se basa en mensajes de texto plano; estos mensajes contienen entre otra información, el número de origen y destino de la llamada. A continuación se detalla el formato de los mensajes SIP con los respectivos datos obtenidos al sondear la red telefónica tanto para mensajes de solicitud como de respuesta.

Mensajes de solicitud.

En la figura 3.15 se indica los datos de la llamada telefónica de ejemplo en un mensaje de solicitud SIP.

LINEA DE SOLICITUD	**Método:** INVITE **Request Url:** sip:022829XXX@172.23.29.4:5060 **Versión:** SIP/2.0
CABECERA	**Via:** SIP/2.0/UDP 200.69.177.17:5060 **Call ID:** 907DF56D@8252b76 **From:**<sip:46044XXX@200.69.177.17:5060> **To:**<sip:022829XXX@172.23.29.4:5060> **Cseq:** 1015313096 INVITE **Contact:**<sip:46044XXX@200.69.177.17:5060> **Content-Length:** 149 **Content-type:** application/SDP **Max Forwards:** 70 **Allow:** INVITE, ACK, CANCEL, BYE, OPTIONS, NOTIFY, UPDATE, INTO, REFER.
LÍNEA EN BLANCO	
CUERPO DEL MENSAJE	**SDP Version Protocol (v):** 0 **SDP owner/creator SessionID (o):**- 0 0 IN IP4 200.25.190.2 **SDP Connection Information (c):** IN IP4 200.25.190.2 **SDP Time Description (t):** 0 **SDP Media Description (m):** Media type: audio Transport Port: 7482 Transport Protocol: RTP/AVP Media Format: 8 101. **SDP Attribute (a):** Attribute: rtpmap Payload type: 101. Encoding name: telephone-event Clockrate: 8000

Figura 3.15Datos de una llamada telefónica en Mensaje de solicitud SIP.

Mensajes de respuesta.

En la figura 3.16 se indica los datos de la llamada telefónica de ejemplo en un mensaje de respuesta SIP.

LINEA DE ESTADO	**Código del estado:** 200 OK. **Versión:** SIP/2.0
CABECERA	**Via:** SIP/2.0/UDP 200.69.177.17:5060 **Call ID:** 907DF56D@8252b76 **From:**<sip:46044XXX@200.69.177.17:5060> **To:**<sip:022829XXX@172.23.29.4:5060> **Cseq:** 1015313096 INVITE **Contact:**<sip:022829XXX@172.23.29.4:5060> **Content-Length:** 203 **Content-type:** application/SDP
LÍNEA EN BLANCO	
CUERPO DEL MENSAJE	**SDP Version Protocol (v):** 0 **SDP owner/creator Session ID (o):**HuaweiSoftX3000 4562236 4562237 IN IP4 172.23.29.4 **SDP Connection Information (c):**IN IP4 172.23.29.4 **SDP Time Description (t):** 0 **SDP Media Description (m):** Media type: audio Transport Port:42054 Transport Protocol: RTP/AVP Media Format: 8 101. SDP Attribute (a): Attribute: rtpmap Payload type: 8 Encoding name: PCA Clock rate: 8000

Figura 3.16 Datos de una llamada telefónica en Mensaje de respuesta SIP

Campos de Hora/Fecha de Inicio/Fin de llamada.

PANTERA 100, es un equipo destinado a sondear señalización en tiempo real; es decir que los datos obtenidos para hora y fecha de inicio y fin de llamada son capturados el momento exacto en el cual se estableció la llamada telefónica, obteniendo de esta forma los campos mencionados del CDR con una gran precisión.

Duración de llamada.

Para que se genere una llamada telefónica, es necesario que exista un flujo de gestión y establecimiento de la misma. Al tener información de los intervalos de tiempo en los que se efectuó cada uno de las partes de este proceso, podemos determinar el tiempo de duración total de la llamada telefónica. Para el ejemplo se obtuvo los siguientes datos con respecto a los tiempos como indica la figura 3.17.

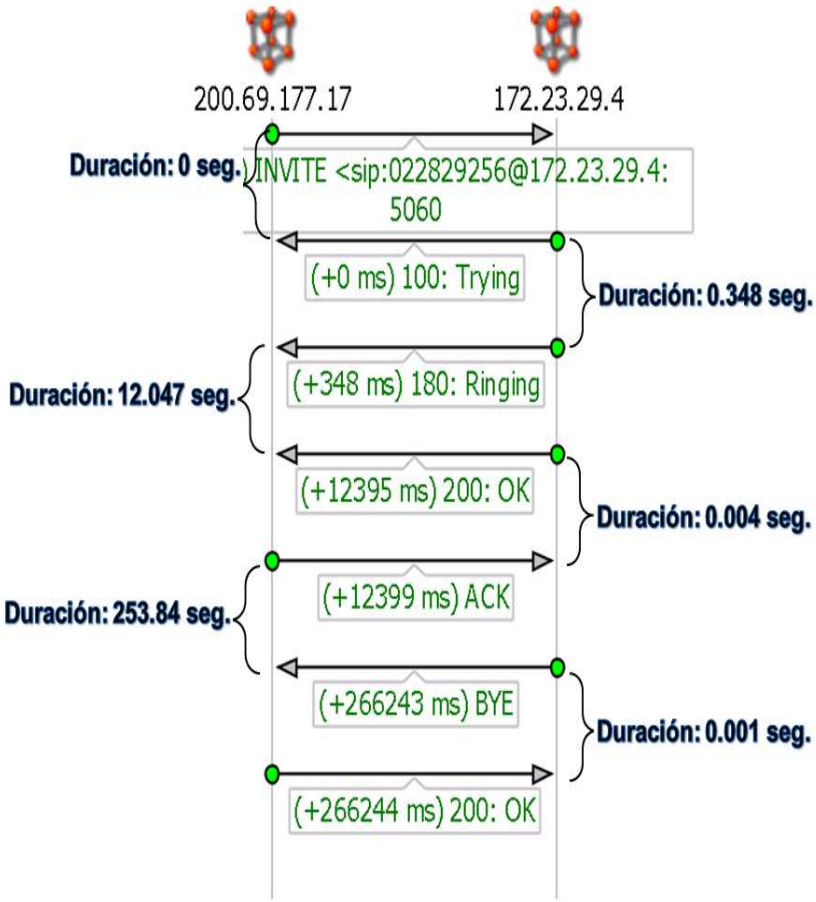

Figura 3.17 Establecimiento de una llamada telefónica mediante SIP.

Cada uno de estos intercambios de mensajes entre usuarios de origen y destino se los realiza en un determinado tiempo. Al obtener el tiempo de las transferencias de cada uno de los mensajes podemos determinar la duración total de la llamada, lo cual se resume en la tabla 3.4.

Mensaje	Descripción	Duración (segundos)
Invite	Envío de petición de inicio de llamada.	0
Trying	Mensaje de respuesta al invite anterior	0.348
Ringing	Alerta al usuario destino de la llamada. Se envía un mensaje al llamante de la situación actual, en este caso: timbrando.	12.047
OK	Petición de inicio de llamada aceptada	0.004
ACK	Confirmación de respuesta. Duración de la conversación	253.84
BYE	Petición de terminación de llamada	0.001
OK	Terminación de llamada aceptada	Fin de llamada.
Tiempo total de gestión de llamada		**12.4**
Tiempo total propiamente de llamada		**253.84**
Duración Total.		**266.24**

Tabla 3.4 Tiempos de duración de una llamada mediante SIP

3.5 BASE DE DATOS PARA LOS CDRs.

Una base de datos es la recopilación de una gran cantidad de información organizada de tal manera que se pueda tener acceso a datos específicos mediante cadenas de consultas.

Generalmente la información está organizada por: campos, registros y archivos. Un campo es un fragmento único de información; un registro es un conjunto de todos los campos; y un archivo es una recopilación de registros. En una base de datos existen varias tablas que contienen información que está relacionada entre ellas. En la figura 3.18 se indica un ejemplo de una tabla perteneciente a una base de datos con sus respectivos elementos.

Figura 3.18Elementos de una tabla

3.5.1 GENERACIÓN DE LA BASE DE DATOS.

Para el presente Proyecto, se importa la información obtenida de la sonda de señalización hacia una base de datos creada en Microsoft Access; de tal forma que se pueda extraer datos específicos sobre ciertos campos de los CDRs, con la finalidad de identificar posibles escenarios de fraude dentro del servicio de telefonía fija que brinda la Corporación Nacional de Telecomunicaciones.

A continuación se explica detalladamente el proceso para generar la base de datos, que se usará específicamente para este Proyecto.

3.5.1.1 Creación de una nueva base de datos.

El primer paso es crear una nueva base de datos; para ello se elige base de datos en blanco con el nombre que se desea como indica la figura 3.19.

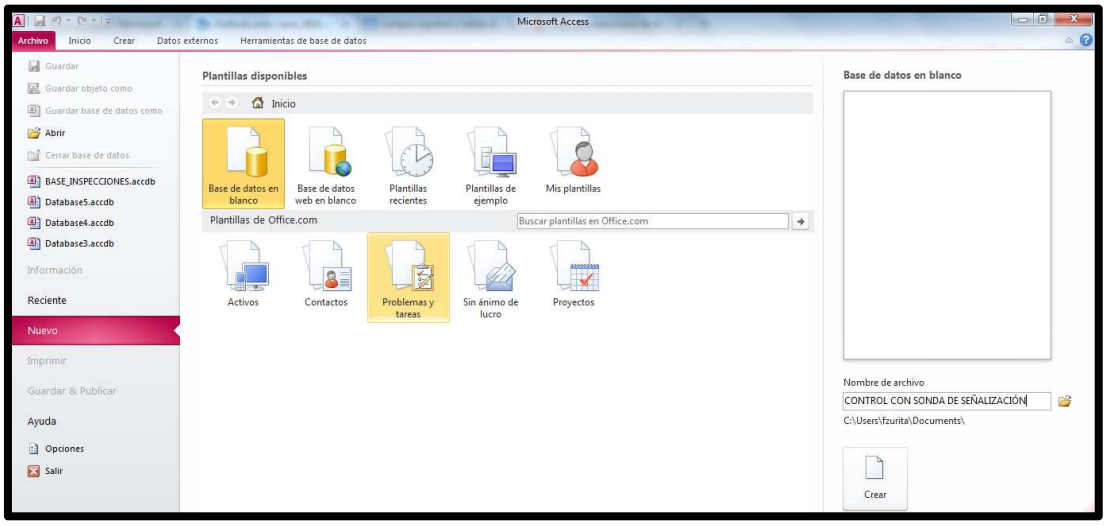

Figura 3.19 Creación nueva base de datos

3.5.1.2 Importación de datos externos hacia la base de datos.

Para importar datos externos se selecciona en el caso de este proyecto la opción Importar Archivos de Texto, inmediatamente se despliega la pantalla que se muestra en la figura 3.20.

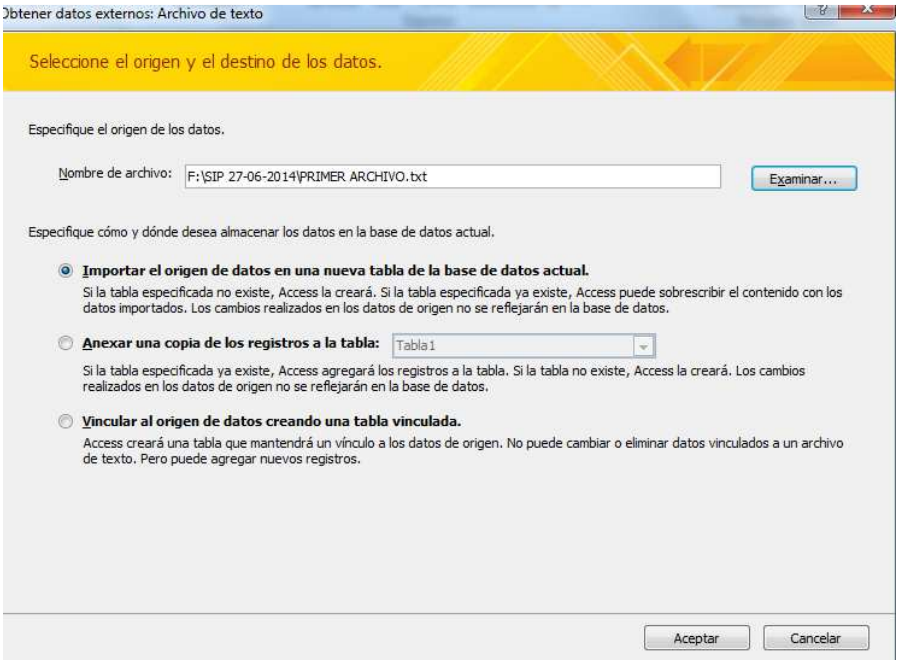

Figura 3.20 Importación de datos externos.

Dentro de esta pantalla existe una opción en la cual se puede examinar la ubicación del archivo de texto que se quiere importar.

A continuación se despliega una nueva ventana como la que se muestra en la Figura 3.21.

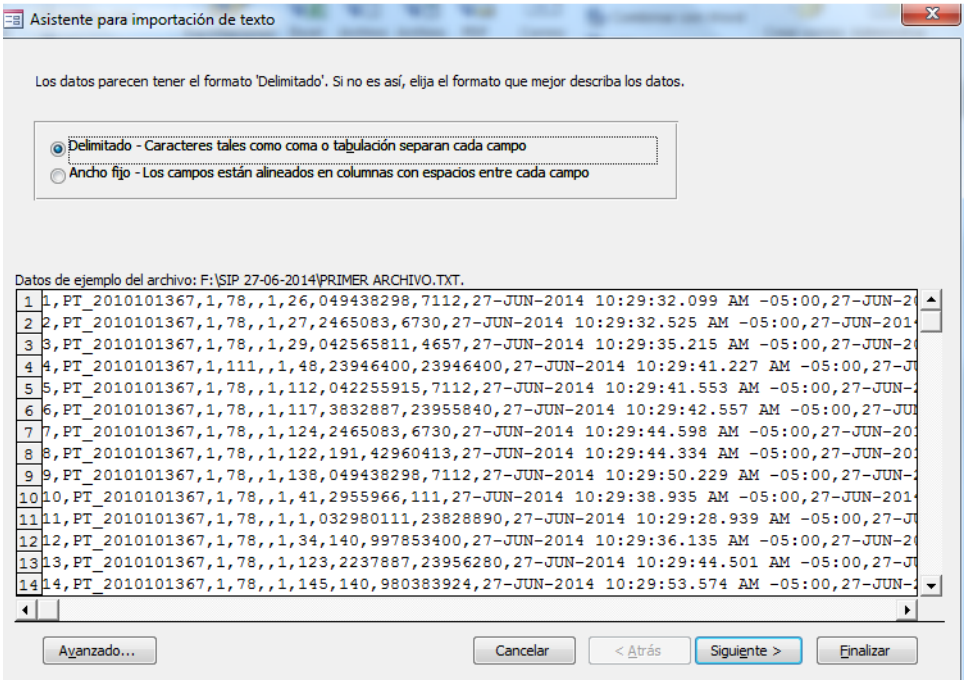

Figura 3.21 Configuración de importación de archivos externos

Dentro de esta ventana se elige el formato en el cual están organizados los datos de los archivos de texto a ser importados. En este caso se escoge la opción delimitado porque los campos de los archivos que genera la sonda de señalización están separados por comas. Posteriormente se selecciona el ícono Avanzado para configurar la especificación de importación.

Dentro de la ventana Especificación de importación, que se muestra en la figura 3.22, existen varias opciones que se puede configurar, de las cuales las más importantes son:

- Delimitador de campo.
- Delimitador de fecha.
- Delimitador de hora.
- Símbolo decimal.

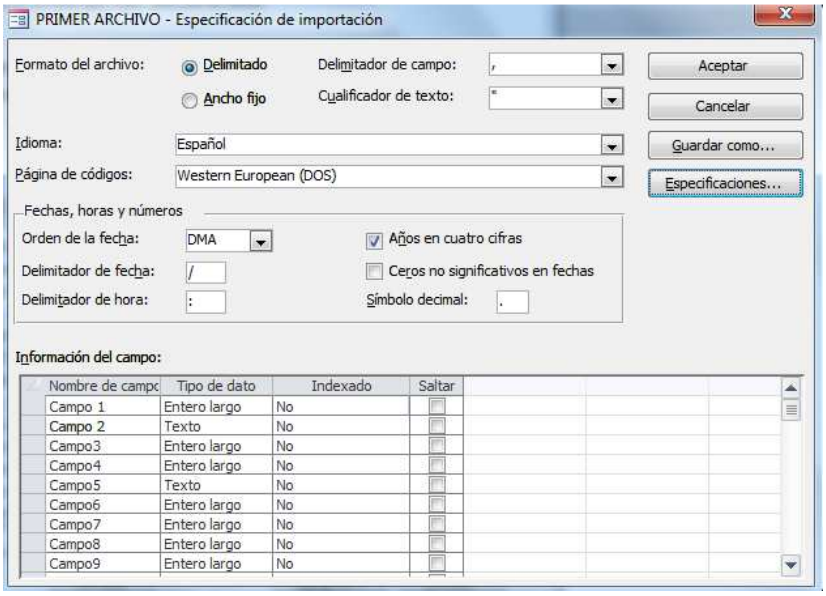

Figura 3.22 Configuración de especificación para importar datos.

Dentro de esta ventana también se puede dar el nombre correspondiente a cada uno de los campos y determinar el tipo de dato para cada uno de éstos. Además existen campos que no son de interés para las posteriores consultas de la base de datos; para ello existe la opción saltar y de esta forma suprimir campos determinados. En la figura 3.23 se observa la figura en la que se puede realizar la configuración de cada uno de los campos de los CDRs.

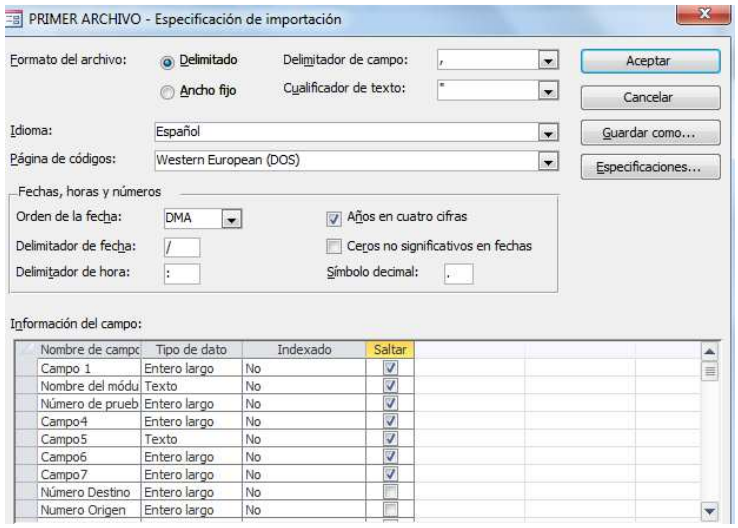

Figura 3.23 Configuración de los campos

Posteriormente se guarda la especificación con el nombre que se desee como se muestra en la figura 3.24

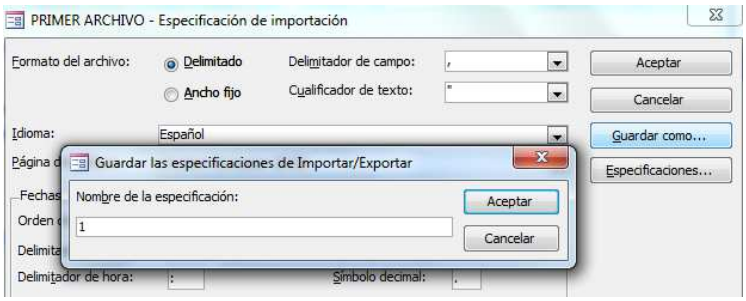

Figura 3.24 Proceso de guardado de la especificación.

Se importa el archivo a una tabla con un nombre que el usuario determina como se indica en la figura 3.25

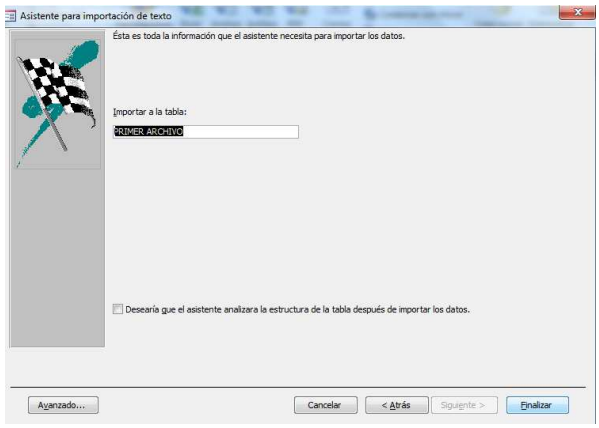

Figura 3.25 Asignación de nombre de tabla creada.

Finalmente se tiene la tabla perteneciente a la base de datos como indica la figura 3.26.

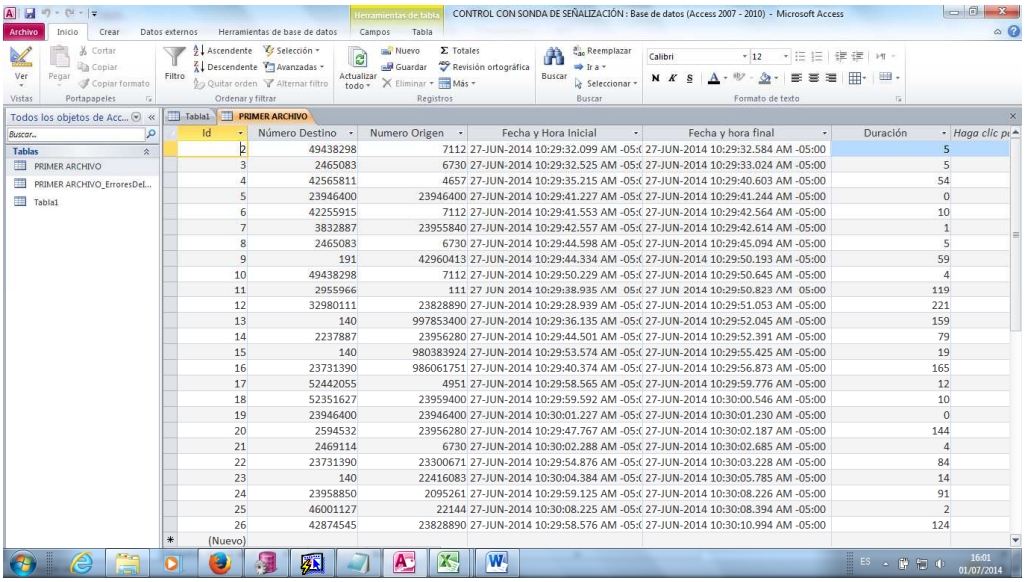

Figura 3.26 Tabla obtenida mediante la importación de archivos de texto.

3.5.1.2.1 Importación simultánea de varios archivos de texto.

Puesto que existen numerosos archivos de texto que genera la sonda dentro de un día, resulta muy complicado importar archivo por archivo, por ello se creó un script en Visual Basic para poder importar automáticamente los diferentes archivos dentro en una misma tabla. El código fuente se muestra en la figura 3.27.

```
Option Compare Database

'---------------------------------------------------------------
' IMPORTARTEXTO
'
'---------------------------------------------------------------
Function IMPORTARTEXTO()
On Error GoTo IMPORTARTEXTO_Err

    DoCmd.TransferText acImportDelim, "1", "PRIMER DIA", "F:\SIP 27-06-2014\PRIMER ARCHIVO.txt", False, ""
    DoCmd.TransferText acImportDelim, "1", "PRIMER DIA", "F:\SIP 27-06-2014\SEGUNDO ARCHIVO.txt", False, ""
    DoCmd.TransferText acImportDelim, "1", "PRIMER DIA", "F:\SIP 27-06-2014\TERCER ARCHIVO.txt", False, ""
    DoCmd.TransferText acImportDelim, "1", "PRIMER DIA", "F:\SIP 27-06-2014\CUARTO ARCHIVO.txt", False, ""
    DoCmd.TransferText acImportDelim, "1", "PRIMER DIA", "F:\SIP 27-06-2014\QUINTO ARCHIVO.txt", False, ""
IMPORTARTEXTO_Exit:
    Exit Function

IMPORTARTEXTO_Err:
    MsgBox Error$
    Resume IMPORTARTEXTO_Exit

End Function
```

Figura 3.27 Script para importación simultánea de archivos de texto

Después de ejecutar el script, se tiene como resultado una tabla con los datos de todos los archivos de texto que la sonda de señalización generó en un día como se indica en la figura 3.28.

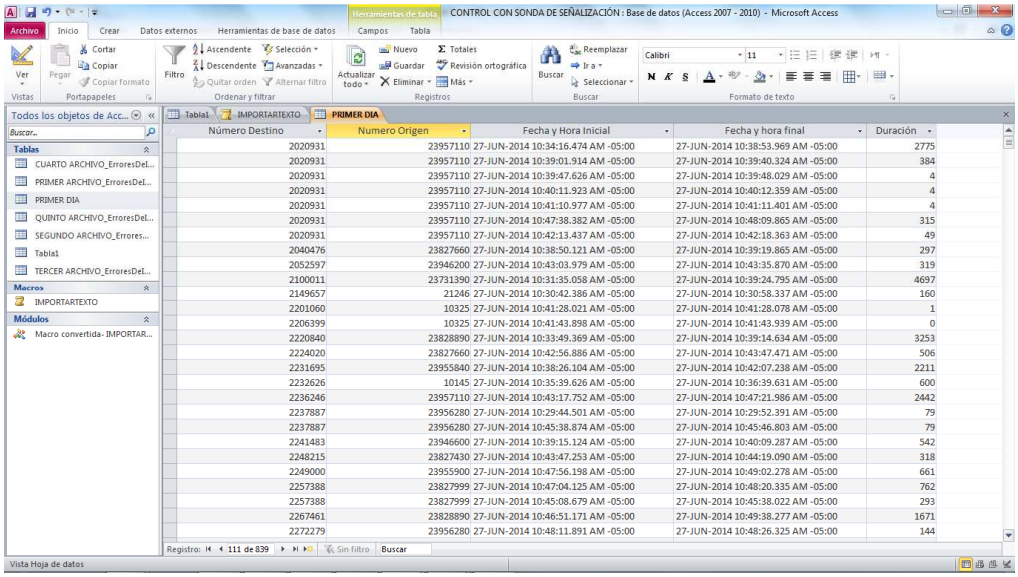

Figura 3.28 Tabla obtenida mediante la importación simultánea de varios de archivos de texto.

CAPÍTULO 4.

DETECCIÓN DE POSIBLES USOS INDEBIDOS DEL SERVICIO DE TELEFONÍA FIJA EN CNT MEDIANTE EL ANÁLISIS DE LOS CDRS.

4.1 INTRODUCCIÓN.

Dentro de los servicios de telefonía fija que prestan las empresas de Telecomunicaciones, es de gran importancia realizar un control del tráfico telefónico para lograr identificar posibles usos indebidos del servicio que pueden representar potenciales escenarios de fraude. El método que se implementó para lograr detectar comportamientos atípicos en las líneas de telefonía, se basa en el análisis de los registros de llamada conocidos como CDRs, los cuales contienen diferentes campos de información como son: origen, destino, fecha de la llamada, hora de inicio de la llamada, hora de finalización de llamada, duración, tipo de llamada entre otros. En función de detectar posibles fraudes, se establecieron valores umbrales para varios de estos campos. Si al analizar los CDRs se observan valores superiores a los umbrales, se genera una alarma, que debe ser tomada en cuenta para confirmar si existe una actividad fraudulenta. Cuando surge una alarma se realiza un análisis diferencial, en el cual se monitorean patrones de comportamiento de la línea telefónica comparando sus más recientes actividades con la historia de uso de la misma; un cambio en el patrón de comportamiento permitirá detectar escenarios fraudulentos.

Enuncontrol de tráfico telefónico efectuado para identificar fraudes, existe un término muy importante llamado falso positivo. Un falso positivo se genera cuando a pesar de existir una alarma de un posible fraude, el analista determina que no lo es después de un análisis minucioso.

El presente proyecto tiene como finalidad obtener los mencionadosCDRs a bajo nivel; es decir sondeando protocolos de señalización: SIP y SIGTRAN dentro de la red telefónica de la Corporación Nacional de Telecomunicaciones como se indica en la figura 4.1.

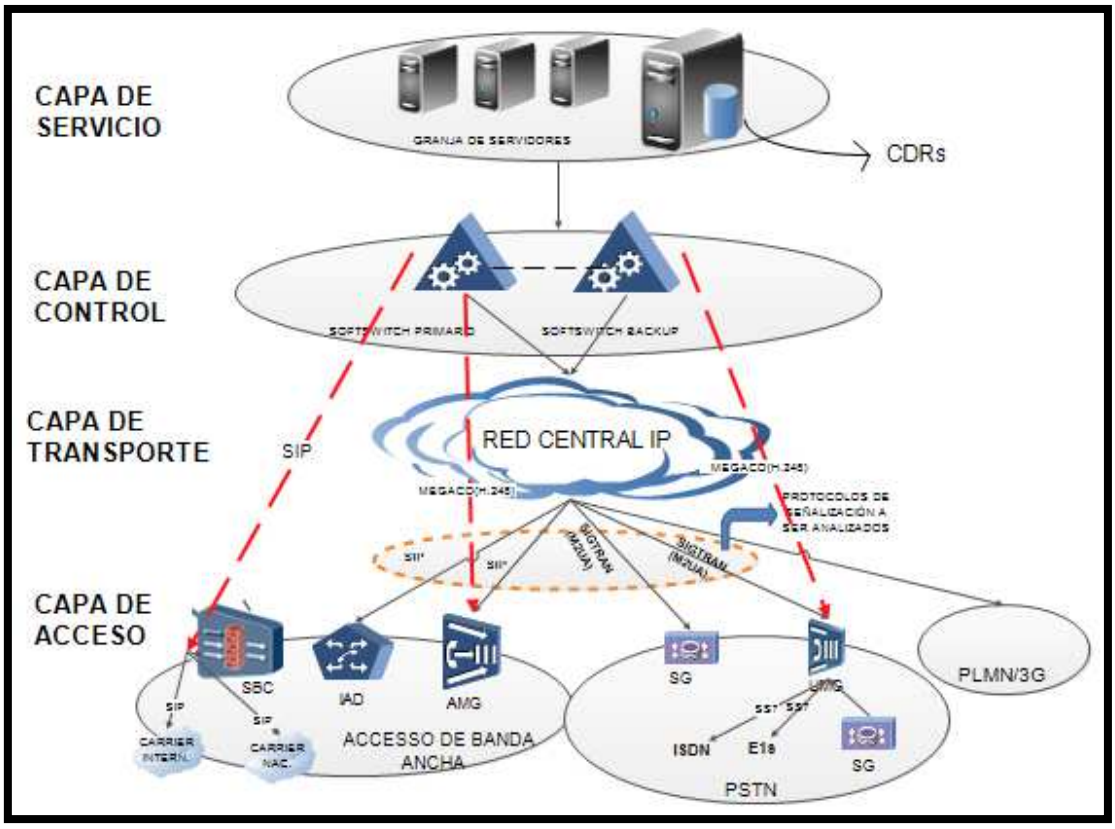

Figura 4.1 Diagrama General de la red de telefonía de CNT.

4.2 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE CLIP ON.

4.2.1 PATRÓN DE COMPORTAMIENTO.

Existe un patrón de comportamiento habitual en las líneas de telefonía fija mediante las cuales se realiza el denominado fraude Clip On o Robo de Líneas.Este comportamiento se basa en la realización de llamadas, generalmente a destinos celulares e internacionales; las llamadas son de larga duración efectuadas en altas horas de la noche con la finalidad de que el defraudador no sea descubierto por el dueño de la línea telefónica al coincidir en la utilización de la misma. Otro indicador importante es la presencia de llamadas hacia destinos nunca antes realizados bajo las condiciones anteriormente descritas.

En la figura 4.2 se indica el comportamiento de una línea telefónica con fraude Clip On.

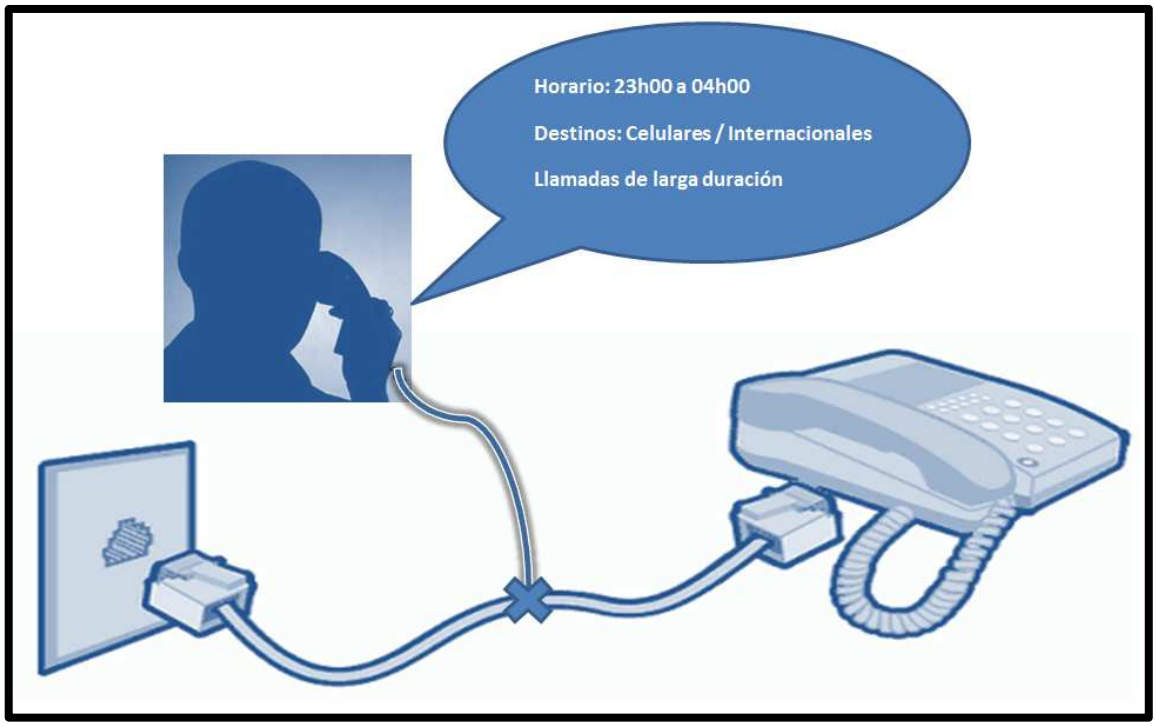

Figura 4.2 Comportamiento Fraude Clip On.

4.2.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS.

Según el patrón de comportamiento descrito anteriormente, los campos de los CDRs a ser considerados para este tipo de fraude son:

- Número origen.
- Número destino.
- Fecha de inicio.
- Fecha de fin.
- Hora de inicio.
- Hora de fin.
- Duración.

Para algunos de estos campos fue factible establecer valores umbrales después de realizar varias pruebas del control para este tipo de fraude. En otros campos del CDR únicamente se estableció algún tipo de restricción que ayude a optimizar las cadenas de consultas. En la tabla 4.1 se detalla estos valores y restricciones con la respectiva justificación.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números de Pichincha.	En el Softswitch de Quito se registran todas las llamadas telefónicas entrantes y salientes de la red de telefonía fija de CNT; incluidos como números de origen de llamada números internacionales, celulares y provinciales. Por esta razón es necesario restringir el número origen solo a la provincia de Pichincha.
Número de destino	Ninguno	Destinos internacionales y celulares	En el fraude Clip On, el defraudador generalmente trata de sacar el mayor provecho de la línea telefónica a la cual está estafando; por ello es muy común que realice llamadas hacia destinos celulares e internacionales que tiene una tarifa más alta en el mercado de la telefonía.
Fecha inicio	Ninguno	Ninguno	Parámetro modificable.
Fecha Fin	Ninguno	Ninguno	Parámetro modificable.
Hora de inicio	23h00 a 04h00	Ninguno	El defraudador prefiere realizar llamadas dentro del horario indicado para evitar ser descubierto por el dueño de la línea telefónica al coincidir en el uso de la misma.
Hora de fin	23h00 a 04h00	Ninguno	El defraudador prefiere realizar llamadas dentro del horario indicado para evitar ser descubierto por el dueño de la línea telefónica al coincidir en el uso de la misma.

Tabla 4.1 Umbrales - Restricciones de campos para Fraude Clip On.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Duración	Llamadas con duración mayor a 1 hora	Ninguno	Generalmente en este tipo de fraude, las llamadas realizadas son de larga duración. Después de varias pruebas y en base al monitoreo de patrones de uso de la línea telefónica; se estableció como valor umbral para la duración de las llamadas una hora.

(Continuación)Tabla 4.1 Umbrales - Restricciones de campos para Fraude Clip On.

4.2.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE CLIP ON.

Una vez conformada la base de datos, se procede a realizar la consulta en lenguaje de consulta estructurado SQL, que permita identificar potenciales líneas telefónicas, mediante las cuales se esté realizando fraude Clip On. Para la elaboración de la consulta se tomó en consideración los campos de los CDRs, que se mencionó anteriormente, con sus respectivos valores umbrales y restricciones de la siguiente manera:

- Teléfonos origen: Las líneas telefónicas a ser analizadas corresponden únicamente a la provincia de Pichincha; por ello en el código fuente se incluyó una restricción para consultar solo números de origen que empiecen con 2 o 02.
- Teléfonos destinos: Internacionales y celulares. Dentro del código fuente se analizarán todos los números destino, excepto los que comiencen con 02, 03, 04, 05, 06, 07, 2, 3, 4, 5, 6, 7, 1 (llamadas a números especiales), 0034 (destino internacional típico: España), 0039 (destino internacional típico: Italia), 911 (llamadas de emergencia).
- Hora de inicio y fin de llamada:Dentro del horario de 23h00 a 04h00.
- Duración de llamada: Mayor a una hora. El tiempo en los archivos de texto viene en segundos multiplicado por 10; por lo cual en el código fuente de la consulta se restringe llamadas mayores a 36000.

- Otro parámetro importante a tomar en cuenta en la consulta es el número de llamadas realizadas a diferentes destinos; para este tipo de fraude basta con que exista una sola llamada que reúna las características anteriormente descritas para ser considerada para un análisis posterior.

Finalmente se realizó el código fuente para este tipo de fraude de acuerdo al siguiente diagrama de flujo mostrado en la figura 4.3.

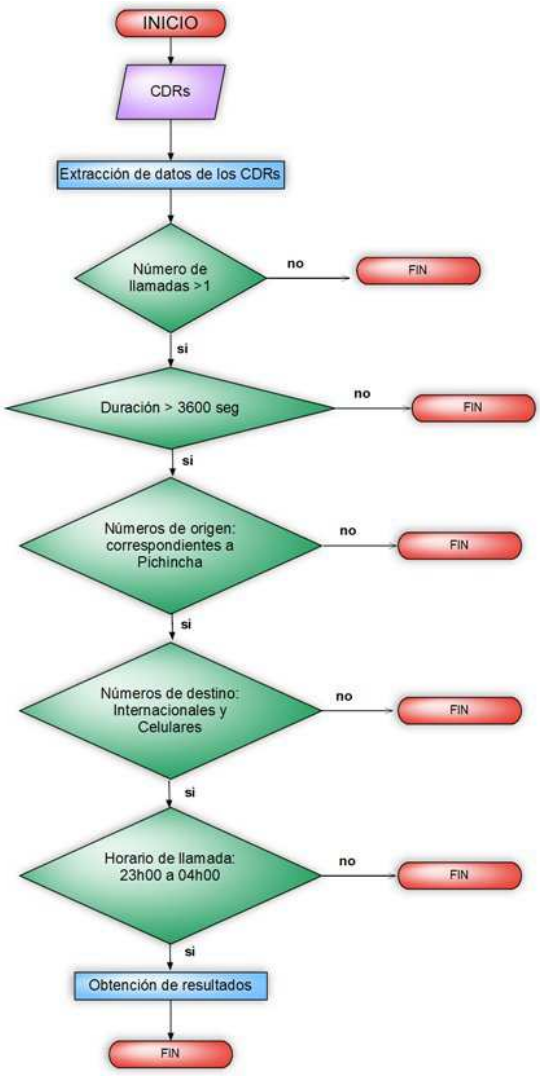

Figura 4.3 Diagrama de flujo para fraude Clip On

En el anexo I se puede observar detalladamente el código fuente para esta consulta.

4.2.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE CLIP ON.

Después de ejecutar la consulta anteriormente descrita, para diferentes fechas en las cuales se tomó señalización; se obtuvo como resultado 56 líneas telefónicas para las cuales se realizará un perfilamiento de tráfico telefónico para determinar la presencia o ausencia de fraude Clip On en las mismas. En la tabla 4.2 se observan los números de estas líneas telefónicas.

224941XX	228890XX	224704XX
220221XX	228976XX	224712XX
220234XX	228995XX	224733XX
220250XX	229201XX	224736XX
220340XX	229232XX	224766XX
220401XX	229244XX	224784XX
222462XX	229777XX	224797XX
222627XX	232628XX	224814XX
222653XX	232640XX	224842XX
222657XX	232802XX	224930XX
222672XX	232815XX	224946XX
222900XX	232827XX	224947XX
222918XX	234001XX	225912XX
222944XX	234009XX	225942XX
222952XX	234022XX	225998XX
223704XX	234436XX	228089XX
224120XX	239620XX	228107XX
224157XX	239621XX	228150XX
224180XX	239708XX	

Tabla 4.2 Números telefónicos resultantes de la consulta.

Posteriormente se procedió a examinarmás detalladamente las líneas telefónicas anteriormente mencionadas, con el objetivo de obtener mayor información acerca de los propietarios de dichas líneas telefónicas. Para ello se utilizó el software computacional perteneciente a la Corporación Nacional de

Telecomunicacionesencargado de llevar un control de la facturación y de operaciones en dicha empresa. Es así que se obtuvo específicamente la siguiente información.

- Datos personales del abonado: cédula de identidad, teléfono de contacto, dirección electrónica, ocupación, etc.
- Ubicación exacta de la línea telefónica.
- Tipo de línea telefónica: residencial o comercial.
- Historial de facturación detallado en meses.
- Historial detallado de reclamos y/o problemas relacionados con el servicio
- Otros servicios adjudicados al abonado.

Una vez considerada esta información, se obtuvo 39 líneas telefónicas para las cuales se debe mantener una señal de alerta. Algunos de los indicativos principales para mantener estas alarmas son: aumento considerable en las últimas cuentas de la facturación, incremento en el historial de uso de la línea telefónica, existencia de numerosas líneas telefónicas con el mismo perfil de comportamiento de uso a nombre del abonado, líneas nuevas con cuentas de facturación sumamente altas en el primer mes de uso (indicativo de un fraude por suscripción). En la tabla 4.3 se detalla los números de las líneas telefónicas que se tomaron en consideración para examinarlas más minuciosamente.

220221XX	224947XX	224157XX
220234XX	225942XX	224180XX
220250XX	225998XX	224704XX
220340XX	228089XX	224712XX
222627XX	228890XX	224733XX
222653XX	228976XX	224736XX
222672XX	229244XX	224766XX
222900XX	229777XX	224784XX
222918XX	232628XX	224797XX
222944XX	232827XX	224814XX
222952XX	234009XX	224842XX
223704XX	234436XX	224930XX
224120XX	239621XX	224946XX

Tabla 4.3Líneas telefónicas a ser examinadas con detalle.

A continuación se procede examinar la totalidad del tráfico telefónico cursado por estas líneas telefónicas con el fin de encontrar patrones de comportamiento

inusuales en las llamadas realizadas y recibidas, algunos de ellos se describen a continuación.

- Llamadas hacia destinos nunca antes registrados en un horario de 22h00 a 04h00.
- Aumento considerable de tráfico telefónico en el horario mencionado. Principalmente hacia destinos internacionales y celulares.
- Llamadas de forma repetitiva hacia un mismo destino, del cual no se registra llamadas entrantes.

Después de tomar en cuenta las consideraciones anteriormente descritas, se obtuvo 21 líneas telefónicas catalogadas aún como posibles medios de un fraude Clip On como indica la tabla 4.4.

220221XX	222900XX	224712XX
220234XX	222918XX	224733XX
220250XX	222944XX	224766XX
220340XX	223704XX	224784XX
222627XX	224120XX	224930XX
222653XX	224157XX	224947XX
222672XX	224704XX	225942XX

Tabla 4.4 Líneas telefónicas a ser contactadas.

En este punto, aún existen líneas telefónicas que generan alerta de la presencia de fraude Clip On, por lo cual el siguiente paso es contactarse con los propietarios de las líneas telefónicas e indagar los motivos por los cuales existió un comportamiento irregular en el uso de la línea; existen dos opciones:

- El abonado admite haber realizado las llamadas telefónicas; por lo cual se cierra el caso de análisis de fraude.
- El abonado manifiesta no haber realizado las llamadas y solicita una posterior inspección de la línea telefónica.

En la realización del presente Proyecto, existieron 11 propietarios de las líneas telefónicas que solicitaron una inspección como indica la tabla 4.5.

220221XX	222944XX
220250XX	224704XX
220340XX	224712XX
222627XX	224766XX
222653XX	224947XX
222672XX	

Tabla 4.5 Líneas telefónicas a ser inspeccionadas.

Finalmente se realizó las inspecciones, encontrando fraude por robo de líneas telefónicas en cuatro de ellas; por lo que se procedió a informar a los abonados y tomar las medidas correctivas en estos casos. En la tabla 4.6 se indica los números de las líneas telefónicas que presentaron fraude Clip On.

220250XX
222672XX
222944XX
224712XX

Tabla 4.6 Líneas telefónicas con fraude Clip On.

4.3 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE PBX.

4.3.1 PATRÓN DE COMPORTAMIENTO.

Las centrales secundarias privadas conocidas como PBX pertenecientes generalmente a empresas, deben tener un alto grado de seguridad en su configuración para evitar la presencia de fraude. En la práctica, existen diferentes procederes por los cuales los defraudadores pueden hacer mal uso de estas centrales con el objetivo de lucrar de forma ilícita. Todos estos métodos reflejan patrones de comportamientos definidos en los cuales existe la presencia de llamadas generalmente hacia destinos internacionales (países inusuales con tarifas telefónicas altas).

Los defraudadores hacen uso de estas líneas telefónicas en horarios fuera de oficina; es decir en horas de la noche y en días no laborables con el fin de realizar el máximo consumo de llamadas sin la posibilidad de ser descubiertos o interrumpidos por el personal administrativo y técnico de la empresa de ser el caso.

Es muy importante aclarar que este tipo de fraude representa un gran impacto en la economía de pequeñas empresas o de suscriptores residenciales; los cuales deben asumir el pago de las llamadas fraudulentas realizadas desde su central privada. Un incremento de tan solo centenas o miles de dólares en la planilla telefónica mensual puede resultar catastrófico para este tipo desuscriptores; es decir que en estas líneas se debe realizar un control minucioso del tráfico telefónico generado por la central PBX con el fin de detectar la presencia de fraude.

En una gran mayoría, los fraudes realizados en las PBX, son efectuados generalmente en aquellas líneas en las cuales existe la presencia de llamadas hacia destinos internacionales muy poco usuales y con tarifas de telefonía altas; con el objetivo de tener un mayor beneficio económico. En la figura 4.4, se puede observar de forma detallada el comportamiento de las líneas telefónicas para este tipo de fraude.

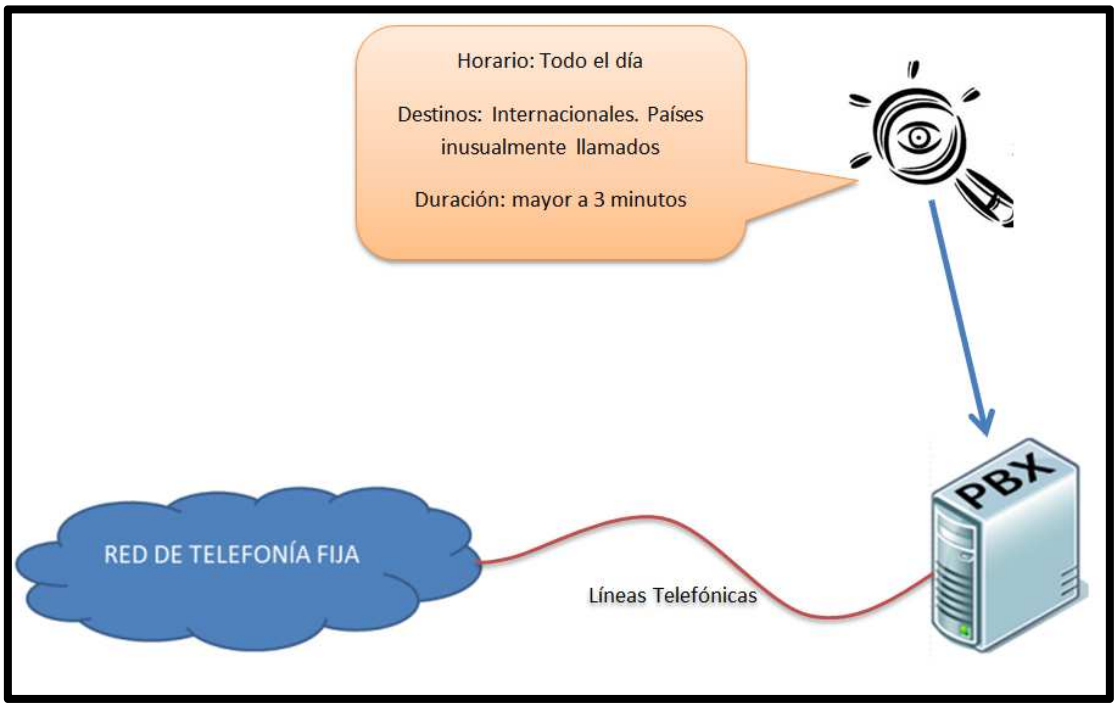

Figura 4.4 Comportamiento Fraude PBX

4.3.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS.

Según el patrón de comportamiento descrito anteriormente, los campos de los CDRs a ser considerados para este tipo de fraude son:

- Número origen.
- Número destino.
- Hora de inicio.
- Hora de fin.
- Duración.

En la tabla 4.7 se detalla los valores y restricciones de estos campos, con la respectiva justificación.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas de Pichincha.	Este tipo de fraude se lo analiza únicamente en los números correspondientes a PBX de empresas o personas particulares.
Número de destino	Ninguno	Destinos internacionales	En este tipo de fraude el principal objetivo es obtener el mayor provecho de las centrales PBX; por ello las llamadas son hechas hacia destinos internacionales poco usuales que tienen una tarifa más alta en el mercado de la telefonía.
Hora de inicio	Todo el día	Ninguno	En fraude de PBX de empresas grandes, solo se necesita tener una llamada hacia destinos internacionales inusuales para tener una señal de alarma.

Tabla 4.7 Umbrales - Restricciones de campos para Fraude PBX.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Hora de fin	Todo el día	Ninguno	En fraude de PBX de empresas grandes, solo se necesita tener una llamada hacia destinos internacionales inusuales para tener una señal de alarma.
Duración	Mayor a 3 minutos	Ninguno	Una llamada con pocos minutos de duración hacia destinos internacionales atípicos es motivo suficiente para un análisis de tráfico telefónico con el propósito de detectar un posible fraude.

(Continuación)Tabla 4.7 Umbrales - Restricciones de campos para Fraude PBX.

4.3.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE PBX.

Este tipo de consulta se basa en un control más estricto mediante el análisis dedestinosinternacionales; explícitamente países a los cuales se realizan muy pocas ocasiones llamadas desde Ecuador. Para la elaboración de la consulta se tomó en consideración los campos de los CDRs que se mencionó anteriormente con sus respectivos valores umbrales y restricciones de la siguiente manera:

- Teléfonos origen: Las líneas telefónicas a ser analizadas corresponden únicamente a líneas de la provincia de Pichincha; por ello en el código fuente se incluyó una restricción para consultar solo números de origen que empiecen con 2 o 02.
- Teléfonos destinos: Dentro del código fuente de la consulta, se decidió analizar como teléfonos destinos únicamente a determinados países. Estos países son destinos a los cuales usualmente no llaman los abonados en Ecuador y que tienen un historial de fraude en PBX. En la tabla 4.8 se detalla un listado de los países destino que en base a la experiencia podrían generar una alarma de un posible fraude a PBX.

DESTINO	PREFIJO	DESTINO	PREFIJO
Bahamas	+1242%	Croacia	+385%
Barbados	+1246%	Finlandia	+385%
Anguila	+1264%	Eslovenia	+386%
Antigua	+1268%	Bosnia	+387%
Bermudas	+1441%	Macedonia	+389%
Grenada	+147%	Rumania	+40%
Turks_Caicos	+1649%	R_Checa	+420%
Monserrat	+1664%	Eslovaquia	+421%
Guam	+1671%	Liechtenstein	+423%
St_Lucia	+1758%	Austria	+43%
Dominica	+1767%	Dinamarca	+45%
St.Vicent&Gren	+1784%	Noruega	+47%
Trinidad y Tobago	+1868%	Polonia	+48%
St_Kitts_Nevis	+1869%	Malvinas	+500%
Jamaica	+1876%	Belice	+501%
Marruecos	+212%	Pedro y Miquelon	+508%
Argelia	+213%	Haiti	+509%
Tunez	+216%	Cuba	+53%
Libia	+218%	Chile Movil	+569%
Gambia	+220%	Guadalupe	+59%
Senegal	+221%	Guyana_Francesa	+592%
Mauritania	+222%	Martinica	+596%
Mali	+223%	Surinam	+597%
Guinea	+224%	Malasia	+60%
Costa_de_Marfil	+225%	Australia_Ter_Ext	+61%
Burkina_Faso	+226%	Indonesia	+62%
Niger	+227%	Filipinas	+63%
Togolesa Rep.	+228%	Nueva_Zelandia	+64%
Benin	+229%	Singapur	+65%
Mauricio	+230%	Tailandia	+66%
Liberia	+231%	Timor Oriental	+670%
Sierra Leona	+232%	Brunei	+673%

Tabla 4.8 Destinos atípicos para fraude PBX.

DESTINO	PREFIJO	DESTINO	PREFIJO
Ghana	+233%	Nauru	+674%
Nigeria	+234%	Tonga	+676%
Chad	+235%	Salomon	+677%
R_Centroafricana	+236%	Vanuato	+678%
Camerun	+237%	Fiji	+679%
Cabo_Verde	+238%	Palaos	+680%
Sao Tome	+239%	Wallis_Futuna	+681%
Guinea_Ecuatorial	+240%	Cook_Islas	+682%
Guinea_Bissau	+245%	Nueva_Caledonia	+687%
Seychelles	+248%	Tuvalu	+688%
Sudan	+249%	Polinesia Francesa	+689%
Ruandesa	+250%	Tokelao	+690%
Etiopia	+251%	Micronesia	+691%
Somalia	+252%	Marshal_Islas	+692%
Djibouti	+253%	Federacion_Rusa	+7%
Kenia	+254%	Corea_del_Sur	+82%
Tanzania	+255%	Vietnam	+84%
Uganda	+256%	Corea_del_Norte	+850%
Burundi	+257%	Macao	+853%
Mozambique	+258%	Camboya	+855%
Zanzibar	+259%	Laos	+856%
Zambia	+260%	Inmarsat	+870%
Madagascar	+261%	Bangladesh	+880%
Reunion	+262%	Iridium	+881%
Zimbabwe	+263%	Taiwan	+886%
Namibia	+264%	Turquia	+90%
Malawi	+265%	India	+91%
Lesotho	+266%	Pakistan	+92%
Botswana	+267%	Afganistan	+93%
Swazilandia	+268%	Sri lanka	+94%
Comorras	+269%	Myanmar	+95%
Sudafrica	+27%	Maldivas	+960%

(Continuación) Tabla 4.8 Destinos atípicos para fraude PBX.

DESTINO	PREFIJO	DESTINO	PREFIJO
Eritrea	+291%	Libano	+961%
Aruba	+297%	Jordania	+962%
Faroe	+298%	Siria	+963%
Groenlandia	+299%	Iraq	+964%
Francia	+336%	Kuwait	+965%
Gibraltar	+350%	Yemen Rep. Arabe	+967%
Luxemburgo	+352%	Oman	+968%
Irlanda	+353%	Palestina	+970%
Islandia	+354%	Emiratos_Arabes	+971%
Albania	+355%	Israel	+972%
Malta	+356%	Bahrein	+973%
Chipre	+357%	Qatar	+974%
Hungria	+36%	Butan	+975%
Lituania	+370%	Mongolia	+976%
Letonia	+371%	Nepal	+977%
Estonia	+372%	Iran	+98%
Moldova	+373%	Tajikistan	+992%
Armenia	+374%	Turkemenistan	+993%
Belarus	+375%	Aserbayana_R.	+994%
Andorra	+376%	Georgia	+995%
Monaco	+377%	Kirgusia	+996%
San_Marino	+378%	Uzbekistan	+998%
Ucrania	+380%	Serbia	+381%

(Continuación)Tabla 4.8 Destinos atípicos para fraude PBX.

- Hora de inicio y fin de llamada: Durante todo el día.
- Duración de llamada: Mayor a tres minutos. El tiempo en los archivos de texto viene en segundos multiplicado por 10; por lo cual en el código fuente de la consulta se restringe llamadas mayores a 1800.

En la figura 4.5 se presenta un diagrama de flujo que permite establecer el código fuente utilizado para la consulta del fraude PBX.

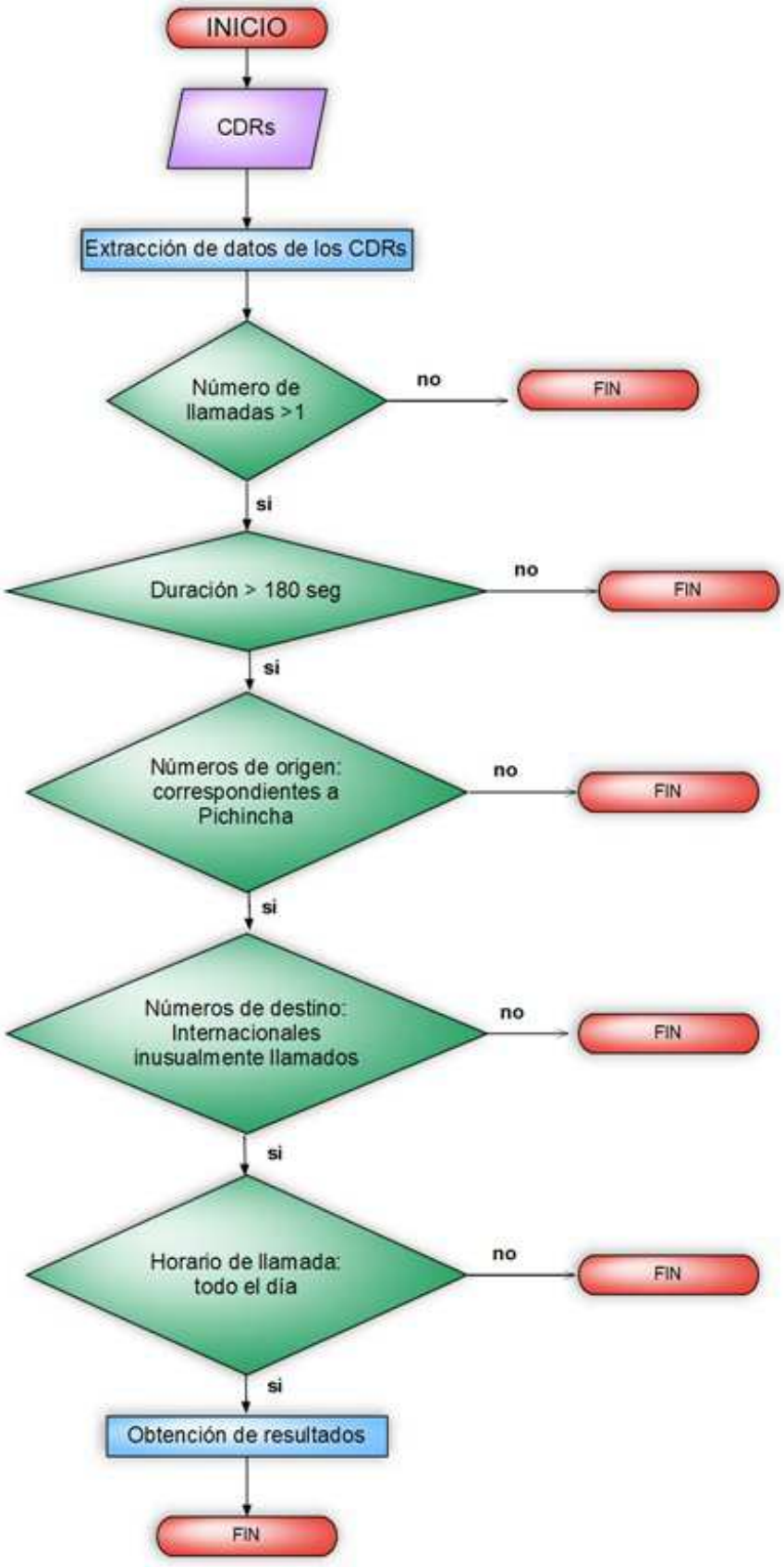

Figura 4.5 Diagrama de flujo para fraude PBX.

En el anexo II, se puede encontrar el código fuente completo de la consulta para este tipo de fraude.

4.3.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE DE PBX.

Dentro de varias fechas se obtuvo seisnúmeros telefónicos asociados a PBX para analizarlos después de ejecutar la consulta diseñada. Estos números telefónicos se los detalla en la tabla 4.9.

229465XX
239725XX
239695XX
239823XX
239663XX
229986XX

Tabla 4.9 Números telefónicos resultantes de la consulta para fraude PBX.

Los números telefónicos resultantes, fueron examinados utilizando el software de control de facturación y operaciones perteneciente a la CNT EP. De esta manera se obtuvo de forma específica la siguiente información.

- Datos de la persona o entidad propietaria de la PBX: cédula de identidad/RUC, teléfono de contacto, dirección electrónica, ocupación/industria, etc.
- Ubicación exacta de la PBX.
- Historial de facturación detallado en meses.
- Historial detallado de reclamos y/o problemas relacionados con el servicio
- Otros servicios adjudicados a la persona o entidad.

Para este tipo de fraude y dentro de los casos en estudio, la información que proporcionó el sistema de control, no fue suficiente como para descartar alguno de los posibles casos de fraude; por lo cual se procede a observar en detalle el tráfico telefónico cursado por estas PBX con el fin de encontrar patrones de comportamiento inusuales en las llamadas realizadas y recibidas, algunos de ellos se describen a continuación.

- Llamadas hacia destinos nunca antes registrados en las noches y fines de semana.

- Aumento considerable de tráfico telefónico. Presencia de llamadas hacia destinos internacionales
- Llamadas de forma repetitiva hacia un mismo país de destino, del cual no se registra llamadas entrantes.

Al finalizar este estudio del tráfico telefónico, tomando en cuenta las consideraciones anteriormente descritas, se obtuvo únicamente dos números telefónicos considerados aún como posibles fraude de PBX; los cuales se detallan en la tabla 4.10.

239695XX
239823XX

Tabla 4.10 Líneas con PBX a ser contactadas.

De estos dos números telefónicos pertenecientes a PBX empresariales, uno de ellos (239823XX) presentaba tráfico telefónico hacia Croacia; aunque es importante aclarar que no se consideraba un problema crítico ya que no existía un número alto de llamadas hacia dicho país. De todas formas se contactó con la empresa perteneciente de la PBX, la cual supo explicar que las llamadas telefónicas fueron realizadas por motivos de desarrollo del negocio y en forma legítima; con lo cual se cerró este caso de análisis de fraude.

El otro número telefónico (239695XX), presentó en el análisis de tráfico telefónico, muchas llamadas hacia Lituania en horarios fuera de oficina. Por esta razón se acordó una reunión con directivos de la empresa propietaria de esta PBX con el objetivo de explicar el problema suscitado y buscar una solución. En esta PBX, se concluyó que fue víctima de fraude, con pérdidas de alrededor de $ 2800 durante dos meses. Cabe recalcar que el manejo y configuración de seguridades de una PBX, es entera responsabilidad del propietario; es así que únicamente se proporcionó recomendaciones para evitar que este problema trascienda.

4.4 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE BYPASS.

4.4.1 PATRÓN DE COMPORTAMIENTO.

Para lograr realizar fraude By Pass, los defraudadores generalmente deben contar con varias líneas telefónicas para finalizar las llamadas internacionales en la red de telefonía de una operadora. Estas líneas telefónicas tienen un patrón de comportamiento en el cual presentan volúmenes de tráfico altos; a su vez no tienen muchas llamadas recibidas.

Un potencial indicativo, de un fraude By Pass, en el comportamiento de las líneas telefónicas es la diversidad y variedad existente de los números telefónicos de destino los cuales son únicamente números locales y nacionales. La duración de las llamadas es media.Todo el comportamiento descrito anteriormente se presenta con una mayor intensidad los fines de semana y días festivos.

En la figura 4.6 se detalla el comportamiento de líneas telefónicas utilizadas en un fraude By Pass.

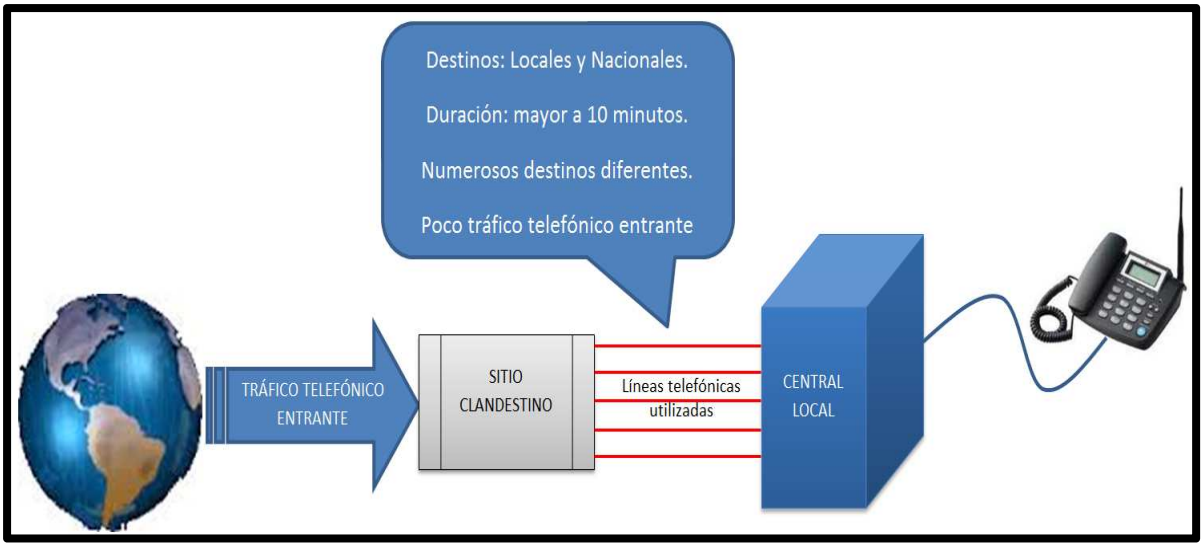

Figura 4.6 Comportamiento de líneas telefónicas usadas en fraude By Pass Entrante

4.4.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS.

Una vez descrito el patrón de comportamiento de las líneas telefónicas utilizadas para realizar fraude By Pass, se consideraron los siguientes campos de los CDRs:

- Número origen.
- Número destino.
- Hora de inicio.
- Hora de fin.
- Duración.

En la tabla 4.11 se detalla los diferentes campos con los respectivos valores umbrales o restricciones.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas de Pichincha.	Solo se analizará líneas telefónicas fijas de la provincia de Pichincha.
Número de destino	Ninguno	Destinos locales y nacionales	En este tipo de fraude se introduce el tráfico telefónico internacional por líneas telefónicas locales y nacionales.
Hora de inicio	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Hora de fin	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Duración	Mayor a 10 minutos	Ninguno	Las llamadas hacia destinos internacionales tienen una duración media aproximada de diez minutos.

Tabla 4.11 Umbrales - Restricciones de campos para Fraude By Pass Entrante.

4.4.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE BY PASS ENTRANTE.

En este tipo de fraude se usan líneas de telefonía fija para ingresar tráfico telefónico internacional en forma de tráfico local. Para la elaboración de la consulta se tomó en consideración los campos de los CDRs que se mencionó anteriormente con sus respectivos valores umbrales y restricciones de la siguiente manera:

- Teléfonos origen: Las líneas telefónicas a ser analizadas corresponden únicamente a líneas de la provincia de Pichincha; por ello en el código fuente se incluyó una restricción para consultar solo números de origen que empiecen con 2 o 02.

- Teléfonos destinos: Para este tipo de fraude, se incluyó en el código fuente de la consulta una restricción para obtener únicamente números de destinos locales y nacionales ya que en un sistema By Pass se introduce el tráfico telefónico internacional por este tipo de líneas telefónicas.

- Hora de inicio y fin de llamada: Durante todo el día.

- Duración de llamada: Mayor a cinco minutos. El tiempo en los archivos de texto viene en segundos multiplicado por 10; por lo cual en el código fuente de la consulta se restringe llamadas mayores a 3000.

- Además existe otro parámetro importante como es el número de llamadas. Para este tipo de fraude se puso como condición que debe existir más de 20 llamadas al día.

En la figura 4.7 se presenta un diagrama de flujo para el diseño del código fuente utilizado para la consulta del fraude By Pass entrante.

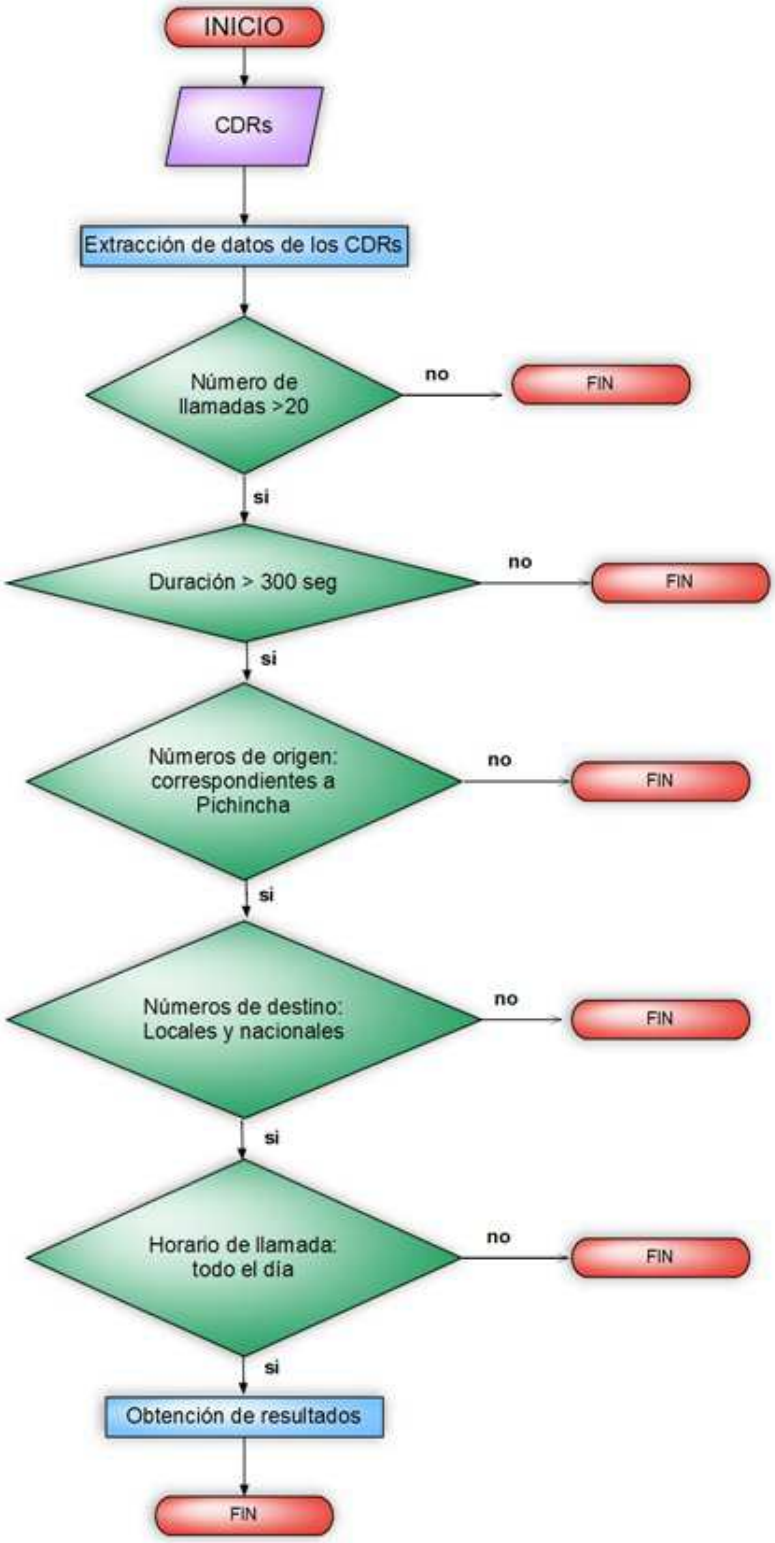

Figura 4.7 Diagrama de flujo para fraude By Pass.

En el anexo III, se puede encontrar el código fuente completo de la consulta para este tipo de fraude.

4.4.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE BYPASS ENTRANTE.

Mediante la ejecución de la consulta, para diferentes fechas en las cuales se tomó señalización; se obtuvo como resultado 25 líneas telefónicas para las cuales se realizará un perfilamiento de tráfico telefónico para determinar si existe o no fraude ByPass. Estas líneas telefónicas se detallan en la tabla 4.12

224773XX	239740XX	239609XX
239721XX	239759XX	239610XX
224780XX	239764XX	239620XX
229439XX	239789XX	239621XX
229700XX	239850XX	239622XX
229777XX	239856XX	239634XX
229789XX	239871XX	239646XX
229881XX	220501XX	239708XX
229952XX		

Tabla 4.12 Líneas telefónicas para posterior estudio.

Como continuación, se realizó un estudio más detallado de las líneas telefónicas anteriormente mencionadas, con el objetivo de obtener mayor información acerca de los abonados propietarios de dichas líneas telefónicas. Para ello se utilizó el software computacional para control de la facturación y de operaciones en CNT. Es así que se obtuvo específicamente la siguiente información.

- Datos personales del abonado: cédula de identidad, teléfono de contacto, dirección electrónica, ocupación, etc.
- Ubicación exacta de la línea telefónica.
- Tipo de línea telefónica: residencial o comercial.
- Historial de facturación detallado en meses.
- Historial detallado de reclamos y/o problemas relacionados con el servicio
- Otros servicios adjudicados al abonado.

Después de tomar en cuenta la información descrita, se determinó que en este caso la gran mayoría de líneas telefónicas estaban definidas como líneas comerciales; lo cual justifica la existencia de tarifas altas de facturación y de altos volúmenes de tráfico generadas por las mismas, el cual se analizará como siguiente etapa.

A continuación se procede a examinar el tráfico telefónico cursado por estas líneas telefónicas con el fin de encontrar patrones de comportamiento inusuales en las llamadas realizadas y recibidas, algunos de ellos se describen a continuación.

- Llamadas hacia numerosos destinos locales y nacionales.
- Altos volúmenes de tráfico telefónico saliente y ausencia de llamadas entrantes.
- Alta cantidad de llamadas telefónicas generadas en un día con una duración mayor a diez minutos.

Al tomar en cuenta todas las consideraciones anteriormente descritas, se pudo observar que todas las líneas telefónicas con categoría comercial presentan volúmenes normales de tráfico entrante y patrones de comportamientos habituales.

Únicamente quedó como señal de alarma una línea telefónica residencial con el número 220501XX. En esta línea telefónica si existía tráfico telefónico entrante, aunque era muy poco relacionado con el tráfico telefónico saliente; este último hacia destinos locales y celulares principalmente.

Con toda la información sobre el caso, se decidió realizar una inspección de la línea telefónica. En esta inspección se logró determinar que el abonado propietario estaba haciendo un mal uso del servicio; ya que se utilizaba la línea telefónica residencial ubicada en un local de negocio. El abonado obtenía beneficios económicos al alquilar dicha línea residencial. Es por ello que este caso se cerró al no encontrar la presencia de fraude ByPass, existiendo únicamente una recategorización de la línea telefónica.

4.5 CONTROL DE TRÁFICO TELEFÓNICO PARA FRAUDE DE TERCER PAÍS.

4.5.1 PATRÓN DE COMPORTAMIENTO.

Para el fraude de Tercer País, el defraudador usa una o varias líneas telefónicas para realizar llamadas hacia destinos internacionales, en especial hacia países de

África. Medio Oriente y Cuba, ya que en ellos se registra antecedentes históricos en este tipo de fraude. El fraude de Tercer País generalmente viene acompañado de un fraude por suscripción, puesto que el estafador adquiere líneas telefónicas, con identidades falsas, mediante las cuales realiza la mayor cantidad de llamadas posibles las 24 horas del día, hasta que estas líneas son suspendidas por falta de pago. También es muy común encontrar este tipo de fraude basado en sistemasBy Pass. En la figura 4.8 se indica el comportamiento de líneas telefónicas implicadas en fraude Tercer País.

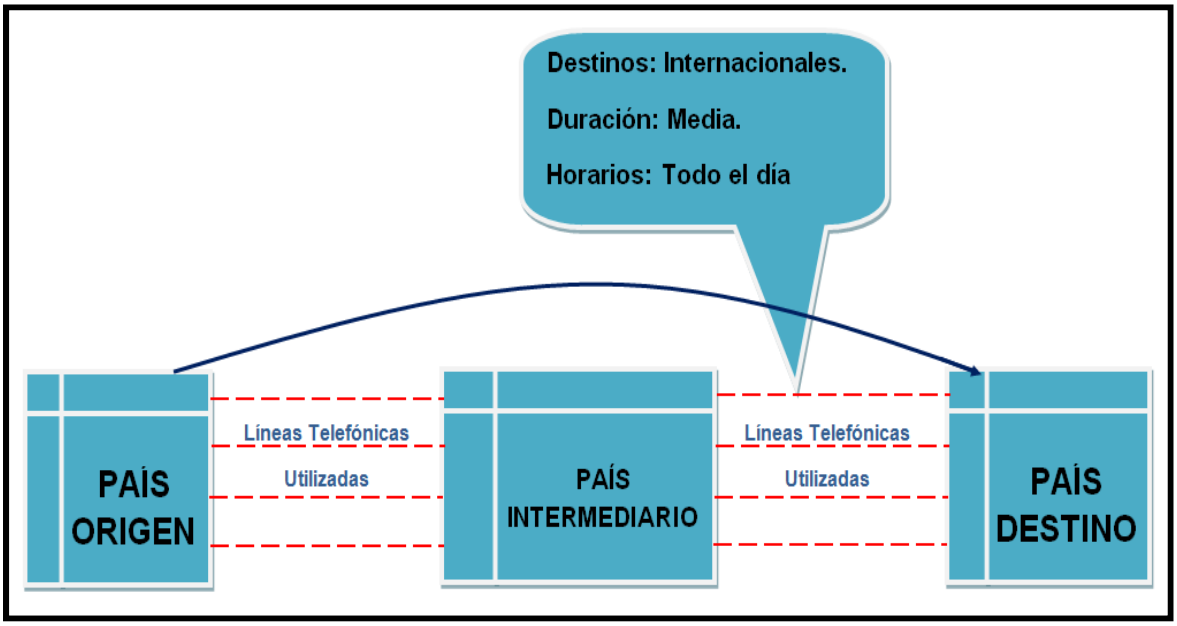

Figura 4.8 Comportamiento Fraude Tercer País

4.5.2 VALORES UMBRALES DE LOS CAMPOS A SER CONSIDERADOS.

Después de realizar la descripción del comportamiento de las líneas telefónicas utilizadas para el fraude de Tercer País, se consideran los siguientes campos de los CDRs:

- Número origen.
- Número destino.
- Hora de inicio.
- Hora de fin.
- Duración.

En la tabla 4.13 se detalla los diferentes campos con los respectivos valores umbrales o restricciones.

CAMPO	VALOR UMBRAL	RESTRICCIÓN	JUSTIFICACIÓN / OBSERVACIÓN
Número de origen	Ninguno	Números correspondientes solo a líneas telefónicas de Pichincha.	El presente proyecto está destinado a analizar fraudes realizados en telefonía fija en la provincia de Pichincha.
Número de destino	Ninguno	Destinos Internacionales	En el fraude de Tercer País, el defraudador generalmente realiza llamadas a destinos internacionales (en especial a Medio Oriente, África y Cuba), para de esta forma sacar el mayor beneficio posible a las líneas telefónicas utilizadas.
Hora de inicio	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Hora de fin	Todo el día	Ninguno	Se analizará el tráfico telefónico generado durante todo el día.
Duración	Mayor a 5 minutos	Ninguno	Las llamadas hacia destinos internacionales tienen una duración media aproximada de cinco minutos.

Tabla 4.13Umbrales - Restricciones de campos para Fraude de Tercer País.

4.5.3 ELABORACIÓN DE LA CONSULTA PARA CONTROL DE FRAUDE DE TERCER PAÍS.

Para la elaboración de la consulta se tomó en consideración los campos de los CDRs que se mencionó anteriormente con sus respectivos valores umbrales y restricciones de la siguiente manera:

- Teléfonos origen: Las líneas telefónicas a ser analizadas corresponden únicamente a líneas de la provincia de Pichincha; por ello en el código fuente se incluyó una restricción para consultar solo números de origen que empiecen con 2 o 02.

- Teléfonos destinos: Internacionales. En la consulta se analizarán todos los números destino, excepto los que comiencen con 02, 03, 04, 05, 06, 07, 09, 2, 3, 4, 5, 6, 7, 9, 1 (llamadas a números especiales), 0034 (destino internacional típico: España), 0039 (destino internacional típico: Italia),911 (llamadas de emergencia) y 001 (destino internacional típico: EEUU).

- Duración de llamada: Mayor a cinco minutos. El tiempo en los archivos de texto viene en segundos multiplicado por 10; por lo cual en el código fuente de la consulta se restringe llamadas mayores a 3000.

- Otro parámetro importante a tomar en cuenta en la consulta es el número de llamadas realizadas a diferentes destinos; para este tipo de fraude deberá existir más de diez llamadasde un mismo número de origen y que reúnan las características anteriormente descritas para ser considerada para un análisis posterior.

En el anexo IV, se detalla el código fuente para la consulta ejecutada en este tipo de fraude.

En la figura 4.9 se presenta el diagrama de flujo que permite obtener el código fuente de la consulta utilizada en fraude de Tercer País.

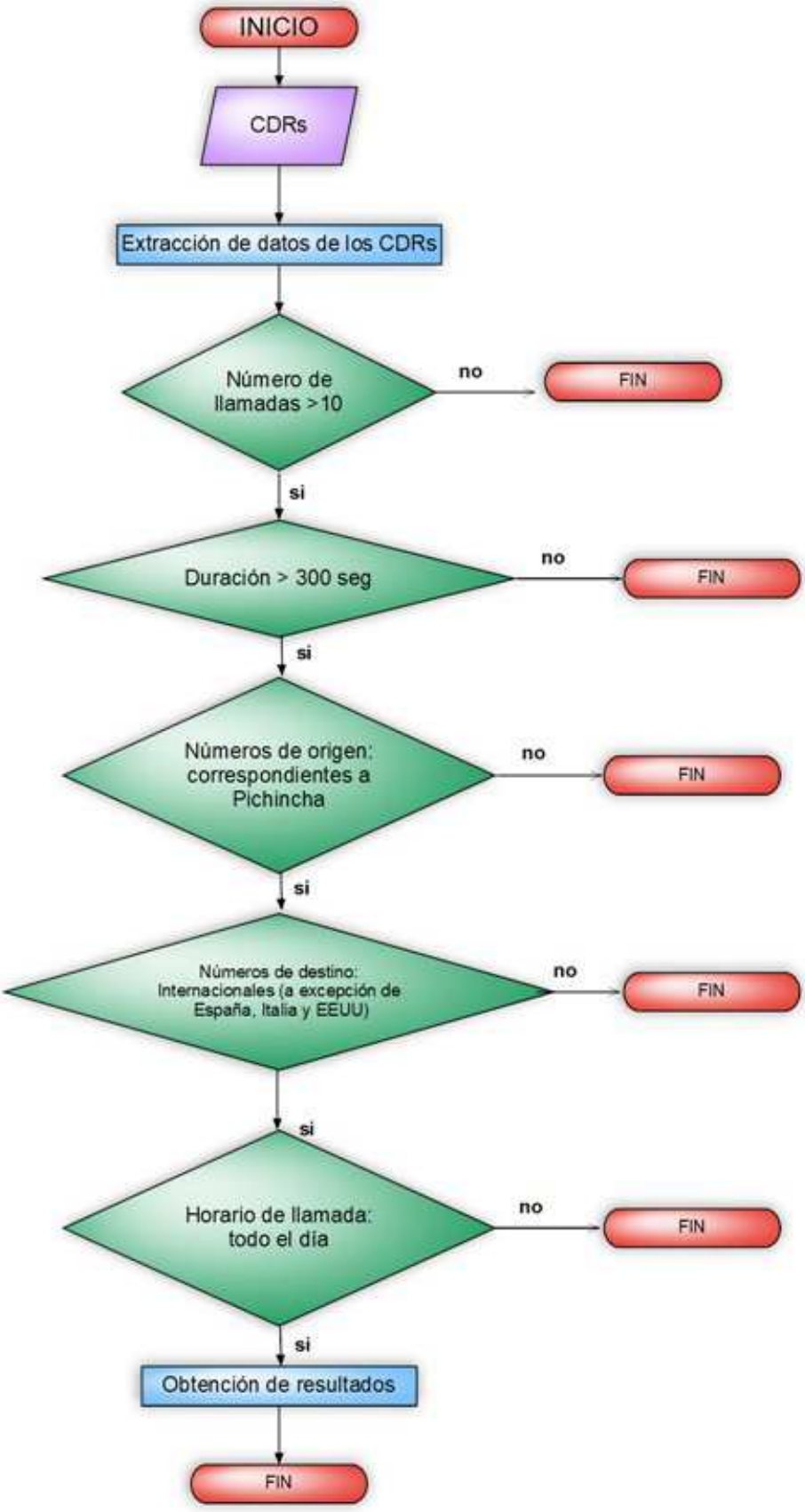

Figura 4.9 Diagrama de flujo para fraude de Tercer País.

4.5.4 OBTENCIÓN DE RESULTADOS PARA FRAUDE DE TERCER PAÍS.

Después de ejecutar la consulta de acuerdo a los parámetros establecidos para la misma, se pudo observar que durante todas las fechas en las cuales se tomó los datos con PANTERA 100, únicamente se generaron como alarmas 3 líneas telefónicas para ser examinadas. Estas líneas telefónicas se detallan en la tabla 4.14.

229777XX
239620XX
239621XX

Tabla 4.14 Líneas Telefónicas a ser examinadas.

Posteriormente se procedió a examinar más detalladamente las líneas telefónicas anteriormente mencionadas, con el objetivo de obtener mayor información acerca de los propietarios de dichas líneas telefónicas. Para ello se utilizó el software computacional encargado de llevar un control de la facturación y de operaciones en CNT. Es así que se obtuvo específicamente la siguiente información.

- Datos personales del abonado: cédula de identidad, teléfono de contacto, dirección electrónica, ocupación, etc.
- Ubicación exacta de la línea telefónica.
- Tipo de línea telefónica: residencial o comercial.
- Historial de facturación detallado en meses.
- Historial detallado de reclamos y/o problemas relacionados con el servicio
- Otros servicios adjudicados al abonado.

Tomando en consideración estos aspectos, se trató de encontrar algunos problemas como son: aumento considerable en las últimas cuentas de la facturación, incremento en el historial de uso de la línea telefónica, existencia de numerosas líneas telefónicas con el mismo perfil de comportamiento de uso a nombre del abonado, líneas nuevas con cuentas de facturación sumamente altas en el primer mes de uso (indicativo de un fraude por suscripción). Se identificó que las líneas telefónicas en análisis correspondían a categoría comercial; sin embargo se observo a detalle el tráfico telefónico entrante y saliente de las

mismas con el fin de encontrar patrones de comportamiento inusuales en las llamadas realizadas y recibidas, algunos de ellos se describen a continuación.

- Llamadas hacia varios destinos internacionales durante todo el día.
- Llamadas de forma repetitiva hacia un mismo país destino, el cual presenta antecedentes históricos en fraude de Tercer País.

Es así que se observó que los volúmenes de tráfico entrante y saliente estaban en rangos normales. Para tener una mayor certeza de que no existe ningún tipo de fraude, se contactó con los propietarios de las líneas telefónicas, quienes confirmaron que las llamadas fueron realizadas desde sus instalaciones de forma legítima, por lo cual se cerraron estos tres casos de análisis de fraude.

Es muy importante aclara que para fraude de Tercer País y Bypass, si se hubiera encontrado presencia de algunos de ellos, la empresa prestadora del servicio conjuntamente con la Superintendencia de Telecomunicaciones realizan operativos para requisar y desmantelar los equipos utilizados para dichos fraudes.

Como resultado finalse pudo determinar que el control de fraude implementado en este Proyecto funciona de forma eficiente,encontrando casos de fraude Clip On y de PBX durante las fechas en las cuales se ejecutó el control. Además los resultados anteriormente descritos, indican que la red telefónica fija de la Corporación Nacional de Telecomunicaciones se encuentra por el momento libre de fraudes como ByPass y Tercer País, lo cual justifica la existencia e importancia del departamento de Prevención de Fraude, así como también de la implementación de controles antifraude en empresas de Telecomunicaciones.

CAPÍTULO 5.

CONCLUSIONES Y RECOMENDACIONES.

5.1 CONCLUSIONES.

- Para poder analizar eficientemente los registros de llamadas telefónicas, obtenidos utilizando el equipo analizador de protocolos; es imprescindible generar una base de datos en la cual se almacenan los campos de los CDRs, pudiendo interactuar con los mismos mediante la programación de cadenas de consultas conocidas como querys en los cuales se establece valores umbrales para varios de estos campos y de esta forma poder extraer información específica para la detección de actividades fraudulentas en telefonía.

- En el presente Proyecto se analizó SIGTRAN; que es un conjunto de protocolos utilizado para transportar señalización SS7 de forma confiable sobre redes IP permitiendo una interoperabilidad entre redes IP de nueva generación y redes SS7 ya existentes. Dentro de este conjunto se encuentra el protocolo M2UA, el cual se lo estudióde forma integralya que es el protocolo utilizado en telefonía fija dentro de CNT. Para ello se analizó, con cierto grado de complejidad, cada una de las capas que conforman la arquitectura SIGTRAN con el objetivo de obtener todos los datos que componen los CDRs

- Los datos que conforman los registros de llamadas, se obtuvieron analizando también el protocolo SIP el cual se basa en mensajes de texto plano que contienen información sobre la llamada entre la cual se destaca como principal: origen y destino, estado de la llamada, tipo de mensaje, trayectoria del mensaje, características de audio y video, entre otra.

- Para la implementación del control de fraude, se utilizó en este Proyecto el método de perfilamiento de una línea telefónica en el cual se analiza la información de las llamadas realizadas por las líneas telefónicas con el objetivo de identificar aquellas que presentan un comportamiento atípico,

indicador de un potencial escenario de fraude. Este método crea perfiles de comportamiento de las líneas de telefonía y establece valores umbrales para los campos de los CDRs como son: número de origen, número de destino, duración de llamada, fecha de inicio y fin de llamada, hora de inicio y fin de llamada.Si existen valores mayores a los umbralles establecidos, se genera una señal de alerta que debe ser considerada por el analista de fraude para examinar las líneas telefónicas mas detalladamente.

- Para analizar si una línea telefónica está siendo usada para algún tipo de fraude en telefonía, es muy importante, además del análisis del tráfico telefónico, que las empresas cuenten con un sistema de control de operación y facturación para poder obtener información más específica como es: datos personales del abonado (cédula de identidad, teléfono de contacto, dirección electrónica, ocupación), ubicación exacta de la línea telefónica, tipo de línea telefónica (residencial o comercial), historial de facturación detallado en meses, historial detallado de reclamos y/o problemas relacionados con el servicio, otros servicios adjudicados al abonado.

- Después de aplicar el control de fraude implementado en este proyecto, se puede concluir que es común encontrar fraude Clip On en líneas telefónicas debido a que es uno de los fraudes más fáciles de realizarlos y no demandan una adquisición previa de infraestructura determinada para realizarlo. Generalmente este tipo de fraude se lo comete vulnerando la acometida externa del servicio, aunque también se puede conectar un cable secundario al cable troncal y llevándolo hacia la ubicación del defraudador siendo este último proceder más complejo.

- El fraude hacia una PBX también está presente debido fundamentalmente a las vulnerabilidades existentes al configurar una PBX sin las debidas normas de seguridad, De acuerdo a la experiencia, este tipo de fraude se lo comete realizando llamadas hacia países de destino inusualmente llamados por los abonados de Ecuador; es por esta razón que el control de fraude PBX implementado se basa en encontrar específicamente llamadas

realizadas desde una PBX hacia países que tienen antecedentes históricos en este tipo de fraude.

- Mediante la aplicación del control de fraude, se puede concluir que la red de telefonía fija de la Corporación Nacional de Telecomunicaciones se encuentra por el momento libre de fraudes como By Pass entrante y Tercer País debido a controles más específicos que se realizan para estos tipos de fraude como es la prueba de lazo cerrado en la cual se genera llamadas internacionales desde el país donde se quiere identificar el fraude hacia líneas terminales que son de propiedad de quien realiza la prueba identificando si la llamada pasó por un carrier autorizado o por un sistema ilegal. La Superintendencia de Telecomunicaciones también ha desempeñado un papel fundamental en la lucha contra sistemas Bypass y fraude de Tercer País realizando operativos para desmantelar estos tipos de sistemas.

- Una vez finalizados la implementación y ejecución del control elaborado en este Proyecto, se puede concluir que los fraudes realizados en telefonía fija pueden llegar a ser causales de pérdidas económicas muy elevadas tanto en líneas comerciales como residenciales; es por esta razón que es muy importante realizar el monitoreo de la red de telefonía en tiempo real y analizar los casos de fraude con la brevedad posible para evitar que las repercusiones económicas sean demasiado altas para los abonados perjudicados.

5.2 RECOMENDACIONES.

- Se recomienda implementar en toda empresa de Telecomunicaciones un control de fraude para telefonía a bajo nivel; es decir basado en el análisis de protocolos de señalización con el objetivo que el mismo sea un control independiente y descentralizado del sistema de gestión utilizado por las empresas.

- Es muy importante tener toda la información detallada correspondiente al servicio de telefonía en una empresa de Telecomunicaciones; por lo cual se recomienda contar con un buen sistema encargado de la gestión y operación del servicio en el cual se pueda encontrar datos específicos sobre las líneas telefónicas y sus abonados.

- Para lograr diseñar un control eficiente a bajo nivel para fraudes en telefonía, se recomienda tener una idea general clara sobre la estructura de la red telefónica y de los protocolos de señalización utilizados en cada etapa de la misma. También es importante contar con el debido sustento teórico de cada uno de estos protocolos, con el fin de poder interpretar correctamente los datos en función de identificar potenciales casos de actividades fraudulentas.

- Se recomienda ejecutar el control implementado en este proyecto diariamente ya que de otra manera se podrían generar grandes pérdidas económicas para las empresas prestadoras del servicio de telefonía, así como también para los suscriptores de las líneas telefónicas.

- Para la elaboración de las consulta de la base de datos, se recomienda utilizar un periodo de prueba para dichas consultas con el fin de que se pueda ajustar, si es necesario, los valores umbrales de los parámetros a ser analizados y tener un sistema de control de fraude eficiente y que no arroje tantos falsos positivos en su análisis.

BIBLIOGRAFÍA

[1] MILLAN, Ramón. RED DIGITAL DE SERVICIOS INTEGRADOS, http://www.ramonmillan.com/tutoriales/rdsi.php. 2008.

[2] JÁCOME, Lorena; VEGA, Martha. "ANÁLISIS Y DISEÑO DE UNA RED IP EN LAS INSTALACIONES DEL ILUSTRE MUNICIPIO DE IBARRA (IMI) CON APLICACIÓN DIRIGIDA A LA TELEFONÍA Y DISEÑO DE UN INFOCENTRO PARA LA PARROQUIA CARANQUI". Escuela Politécnica Nacional. Quito. 2007

[3] SOLÍS, Francisco; VACA, David. "EVALUACIÓN DEL SISTEMA DE TELEFONÍA IP ASTERISK MEDIANTE LA IMPLEMENTACIÓN DE UN PROTOTIPO DE RED EN AMBIENTES IPV4 E IPV6". Escuela Politécnica Nacional. Quito. 2014

[4] Microsoft Corporation. CONCEPTOS DE TELEFONÍA IP. http://msdn.microsoft.com/es-es/library/cc739825(v=ws.10).aspx. 2005

[5] ROCHA, Wiltzer. TELEFONÍA VOIP. http://wilzer-rocha-campos.blogspot.com/2008/09/como-funciona-una-llamada-en-un-sistema.html. 2008.

[6] RENDÓN, Álvaro. SEÑALIZACIÓN EN REDES TELEFÓNICAS. http://dtm.unicauca.edu.co/pregrado/conmutacion/transp/2.4-Senalizacion.pdf.2013

[7] INZIRILLO, Roberto. SEÑALIZACIÓN EN TELEFONÍA. http://www.um.edu.ar/catedras/claroline/backends/download.php.

[8] COIMBRA, Edison. SISTEMAS DE SEÑALIZACIÓN. http://coimbraweb.com/documentos/telecom/9.4_senalizacion_ss7.pdf. 2010.

[9] CUERPO DOCENTE UTFSM, SCTP: Stream Control TransmitionProtocol. http://profesores.elo.utfsm.cl/~agv/elo330/2s11/projects/Reports/BarriosMedinaPerez/index.html.

[10] EFORT. Red de Señalización N° 7.

http://www.efort.com/media_pdf/SS7_ES_EFORT.pdf. 2011.

[11] BLACK, Ulyses. ISDN AND SS7. Primera Edición. Prentice Hall. Estados Unidos. 1997.

[12] Request for Comments 3525. Internet Engineering Task Force (IETF). Gateway Control ProtocolVersion 1. https://tools.ietf.org/html/rfc3525. 2003.

[13] EFORT. PROTOCOLO MEGACO/ H.248. http://www.efort.com/media_pdf/MEGACO_ES_EFORT.pdf. 2011.

[14] BUSTILLO, Antonio; MOLINA, Martín; SÁNCHEZ, Carlos; VILLADIEGO, Claudia. SIGTRAN-SS7 SOBRE IP. Universidad Tecnológica de Bolívar. https://es.scribd.com/doc/73612551/Paper-Sigtran. 2011.

[15] PEREIRA, Javier. SISTEMA DE SEÑALIZACIÓN SIGTRAN. https://eva.fing.edu.uy/pluginfile.php/67122/mod_resource/content/1/20110619_sigtran.pdf. 2011.

[16] Request for Comments 2719. Internet Engineering Task Force (IETF). Network Working Group. Framework Architecture for Signaling Transport. https://www.ietf.org/rfc/rfc2719.txt. 1999.

[17] Request for Comments 4165. Internet Engineering Task Force (IETF). Network Working Group. Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Peer-to-Peer Adaptation Layer (M2PA). https://www.rfc-editor.org/rfc/rfc4165.txt. 2005

[18] TOM, George. M2PA PEER TO PEER ARCHITECTURE. http://www.ietf.org/proceedings/48/SLIDES/sigtran-m2pa/sld002.htm. 2000.

[19] PROTOCOLS.COM.SIGTRAN. http://www.protocols.com/pbook/sigtran.htm

[20] Request for Comments 3331. Internet Engineering Task Force (IETF). Network Working Group. Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) -User Adaptation Layer. http://tools.ietf.org/html/rfc3331. 2002.

[21] ALCATEL USA. M2UA CASE 1 (BACKHAUL) ARCHITECTURE. https://www.ietf.org/proceedings/47/slides/sigtran-peer-00mar/sld003.htm. 2000.

[22] Diseño de una red de señalización SS7 sobre IP para redes de telefonía móvil GSM y UMTS. http://www.dit.upm.es/~enrique/pub/jbento-Memoria.pdf. 2000.

[23] Request for Comments 3332. Internet Engineering Task Force (IETF). Network Working Group. Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -User Adaptation Layer. https://www.ietf.org/rfc/rfc3332.txt. 2002

[24] Request for Comments 4233. Internet Engineering Task Force (IETF). Network Working Group. Integrated Services Digital Network (ISDN)

Q.921-User Adaptation Layer.http://tools.ietf.org/html/rfc4233. 2006

[25] Request for Comments 3868. Internet Engineering Task Force (IETF). Network Working Group. Signalling Connection Control Part User Adaptation Layer (SUA). http://www.ietf.org/rfc/rfc3868.txt. 2004

[26] BOUNURE, Francois; COPPO, Aníbal; CSERNOCH, Diego; Serrano, Daniel. SIP "SESSION INITIATION PROTOCOL". Universidad de Buenos Aires. 2006.

[27] ROJANO, Elio. ACLARANDO CONCEPTOS SOBRE SIP Y VOIP. https://www.sinologic.net/blog/2008-04/aclarando-conceptos-sip-y-voip.html.

2008

[28] MACÍAS, Ignacio; CRUZ, José. TRANSMISIÓN DE VOZ A TRAVÉS DE IP. www.icicm.com/files/Transmision_Voz_IP.doc. 2012

[29] Request for Comments 3261. Internet Engineering Task Force (IETF). Network Working Group. SIP: Session Initiation Protocol.https://www.ietf.org/rfc/rfc3261.txt. 2002

[30] LÓPEZ, Víctor. "ANÁLISIS DE LA PAQUETIZACIÓN DE VOZ SOBRE IP EMPLEANDO EL PROTOCOLO DE INICIO DE SESIONES SIP CON BACK TO BACK USER AGENT (B2BUA) EN UNA APLICACIÓN SOBRE REDES WIFI". Escuela Politécnica del Ejército. Sangolquí. 2011.

[31] PATETE, Luis. EL FRAUDE. http://www.monografias.com/trabajos39/fraude/fraude.shtml#fraude. 2006.

[32] BADILLO, Jorge. AUDITORIA FORENSE. http://www.iaia.org.ar/revistas/elauditorinterno/20/Articulo3.htm. 2008

[33] SUPERTEL. Delitos en Telecomunicaciones.

http://www.supertel.gob.ec/pdf/publicaciones/delitos%20telecomunicaciones%20revista_supertel.pdf. Quito. 2011.

[34] MEZA, María. Dirección General de Investigación Especial en Telecomunicaciones (SUPERTEL). FRAUDE EN TELECOMUNICACIONES. Primera edición. Quito. 2008,

[35] REGLAMENTO GENERAL A LA LEY ESPECIAL DE TELECOMUNICACIONES REFORMADA (Decreto No. 1790). Ecuador. Marzo 2000.

[36] Código Penal. Legislación Conexa. 1ª ed. Corporación de Estudios y Publicaciones. Quito, Ecuador. 1999

[37] Universidad Distrital Francisco José Francisco de Caldas.. TÉCNICAS DE

DETECCIÓN, PREVENCIÓN Y CONTROL DE FRAUDE EN TELECOMUNICACIONES. Colombia. 2004.

[38] ACCANTO SYSTEMS. Manual de sonda de señalización PANTERA 100. Quito. 2011.

GLOSARIO DE TÉRMINOS.

UIT -T	Unión Internacional de las Telecomunicaciones. Sector de normalización de las Telecomunicaciones.
IP	Protocolo de Internet.
TCP/IP	Familia de protocolos. Protocolo de control de transmisión/ Protocolo de Internet.
PCM	Modulación por impulsos codificados.
SIGTRAN	Architectural Framework for Signaling Transport.
SSP	ServiceSwitching Point.
STP	Signal Transfer Point.
SCP	Signal Control Point.
MTP	Media Transfer Protocol.
TDM	Multiplexación por división de tiempo.
IETF	Internet EngineeringTaskForce.
MGC	Media Gateway Controller.
MG	Media Gateway.
UDP	UserDatagramProtocol.
TCP	Transmission Control Protocol.
SCTP	Stream Control TransmissionProtocol.
FSN	Forward SequenceNumber.
BSN	BackwardSequenceNumber.
SG	Gateway de señalización.

ASP	Proceso de servidor de aplicaciones.
ACK	Acuse de recibo.
TEI	Identificador de terminal.
SUA	Signalling Connection Control Part User Adaptation Layer.
IUA	ISDN Q.921 User Adaptation Layer.
SIP	Protocolo de Inicio de Sesiones.
SMTP	Protocolo de Transporte de correo simple.
HTTP	Protocolo de transferencia de Hipertexto.
RSVP	Protocolos de reserva de recursos.
RTP	Protocolo en tiempo real.
SDP	Protocolo de descripción de sesión.
ATM	Modo de transferencia asíncrona.
DISA	Discado Directo Entrante.
PBX	Central Secundaria Privada.
SUPERTEL	Superintendencia de Telecomunicaciones.
CDR	CallDetail Record.
RTX	Sistema Operativo en Tiempo Real.
STM	Módulo de transporte síncrono.
LAN	Red de área local.

ANEXOS

ANEXO I

CONSULTA PARA FRAUDE CLIP ON

```
SELECT *

FROM TABLA_A_CONSULTAR

WHERE NUMERO_ORIGEN IN (SELECT NUMERO_ORIGEN

FROM (SELECT * FROM TABLA_A_CONSULTAR WHERE TABLA_A_CONSULTAR.DURACION>=36000)

GROUP BY NUMERO_ORIGEN

HAVING count(*)>=1) and TABLA_A_CONSULTAR.DURACION>=36000 and (TABLA_A_CONSULTAR.NUMERO_ORIGEN Like "2*" Or TABLA_A_CONSULTAR.NUMERO_ORIGEN Like "02*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "0034*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "0039*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "02*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "03*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "04*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "05*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "06*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "07*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "08*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "911*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "1*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "2*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "3*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "4*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "5*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "6*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO not like "7*") and
```

(TABLA_A_CONSULTAR.NUMERO_DESTINO not like "8*") and (Format(replace(MID(TABLA_A_CONSULTAR.FECHA_INICIO,1,17),"-","/"), "hh:mm") Between "10:00" And "11:59" and (MID(TABLA_A_CONSULTAR.FECHA_INICIO,26,2)="PM"));

ANEXO II

CONSULTA PARA FRAUDE PBX.

SELECT *

FROM TABLA_A_CONSULTAR

WHERE NUMERO_ORIGEN IN (SELECT NUMERO_ORIGEN

FROM (SELECT * FROM TABLA_A_CONSULTAR WHERE TABLA_A_CONSULTAR.DURACION>=1800)

GROUP BY NUMERO_ORIGEN

HAVING count(*)>=1) and TABLA_A_CONSULTAR.DURACION>=1800 and (TABLA_A_CONSULTAR.NUMERO_ORIGEN Like ("2*" or "02*")) and (TABLA_A_CONSULTAR.NUMERO_DESTINO like ("001242*" or "001246*" or "001268*" or "001441*" or "00147*" or "001767*" or "001868*" or "001876*" or "00212*" or "00213*" or "00216*" or "00218*" or "00221*" or "00224*" or "00225*" or "00231*" or "00233*" or "00234*" or "00236*" or "00237*" or "00240*" or "00244*" or "00251*" or "00252*" or "00258*" or "00261*" or "00263*" or "0027*" or "00297*" or "00299*" or "00350*" or "00336*" or "00350*" or "00353*" or "00354*" or "00355*" or "00357*" or "0036*" or "00370*" or "00371*" or "00374*" or "00377*" or "00380*" or "00381*" or "00385*" or "00386*" or "0040*" or "00420*" or "00421*" or "0043*" or "0045*" or "0047*" or "0048*" or "00500*" or "00501*" or "00509*" or "0053*" or "00569*" or "0059*" or "00592*" or "00597*" or "0060*" or "0062*" or "0063*" or "0064*" or "0065*" or "0066*" or "00689*" or "007*" or "0082*" or "0084*" or "00850*" or "00855*" or "00880*" or "00886*" or "0090*" or "0091*" or "0092*" or "0093*" or "0094*" or "00961*" or "00962*" or "00963*" or "00964*" or "00965*" or "00970*" or "00971*" or "00972*" or "00974*" or "00976*" or "00977*" or "0098*" or "00995*" or "00998*" OR "001264*" or "001649*" or "001664*" or "001671*" or "001758*" or "001784*" or "001869*" or "00220*" or "00222*" or "00223*" or "00226*" or "00227*" or "00228*" or "00229*" or "00230*" or "00232*" or "00235*" or "00238*" or "00239*" or "00241*" or "00242*" or "00243*" or "00245*" or "00246*" or "00248*" or "00249*" or "00250*" or "00253*" or "00254*" or "00255*" or "00256*" or "00257*" or "00259*" or "00260*" or "00262*" or

"00264*" or "00265*" or "00266*" or "00267*" or "00268*" or "00269*" or "00291*" or "00298*" or "00352*" or "00356*" or "00372*" or "00373*" or "00375*" or "00376*" or "00378*" or "00382*" or "00387*" or "00389*" or "00423*" or "00508*" or "0059*" or "00596*" or "0061*" or "00670*" or "00673*" or "00674*"or "00675*"or "00676*"or "00677*"or "00678*"or "00679*"or "00680*" or "00681*" or "00682*"or "00683*"or "00684*"or "00685*"or "00686*"or "00687*"or "00688*" or "00690*"or "00691*"or "00692*" or "00853*" or "00856*" or "00870*" or "00881*" or "0095*" or "00960*" or "00688*" or "00967*" or "00968*" or "00973*" or "00975*" or "00992*" or "00993*" or "00994*" or "00996*"));

ANEXO III

CONSULTA PARA FRAUDE BY PASS.

```
SELECT *

FROM TABLA_A_CONSULTAR

WHERE NUMERO_ORIGEN IN (SELECT NUMERO_ORIGEN

FROM (SELECT * FROM TABLA_A_CONSULTAR WHERE TABLA_A_CONSULTAR.DURACION>=3000)

GROUP BY NUMERO_ORIGEN

HAVING count(*)>=20) and TABLA_A_CONSULTAR.DURACION>=3000 and (TABLA_A_CONSULTAR.NUMERO_ORIGEN Like "2*" OrTABLA_A_CONSULTAR.NUMERO_ORIGENLike "02*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO Like "2*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "3*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "4*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "5*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "6*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "7*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "02*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "03*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "04*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "05*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "06*" OrTABLA_A_CONSULTAR.NUMERO_DESTINOLike "07*" );
```

ANEXO IV

CONSULTA PARA FRAUDE DE TERCER PAÍS.

```
SELECT *

FROM TABLA_A_CONSULTAR

WHERE NUMERO_ORIGEN IN (SELECT NUMERO_ORIGEN

FROM (SELECT * FROM TABLA_A_CONSULTAR WHERE TABLA_A_CONSULTAR.DURACION>=3000)

GROUP BY NUMERO_ORIGEN

HAVING count(*)>=10) and TABLA_A_CONSULTAR.DURACION>=3000 and (TABLA_A_CONSULTAR.NUMERO_ORIGEN Like "2*" Or TABLA_A_CONSULTAR.NUMERO_ORIGEN Like "02*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "0034*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "0039*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "02*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "03*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "04*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "05*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "06*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "07*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "08*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "09*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "911*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "1*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "2*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "3*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "4*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "5*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "6*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "7*") and (TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "8*") AND
```

```
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "9*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001202*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001312*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001803*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001614*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001361*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001214*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001313*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001215*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001713*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001702*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001213*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001305*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001212*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "001415*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "0057*") AND
(TABLA_A_CONSULTAR.NUMERO_DESTINO notlike "0051*")
```