ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESARROLLO DE UN SISTEMA BASADO EN ASTERISK QUE PERMITA INVESTIGAR SITUACIONES ANÓMALAS (BYPASS) EN EL ECUADOR PARA LA SUPERTEL

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

JOSÉ GONZALO BÉJAR ALBÁN
E-mail: josebejar87@hotmail.com

DIRECTOR: ING. XAVIER CALDERÓN, M.Sc.
E-mail: xavier.calderon@epn.edu.ec

Quito, julio de 2011

DECLARACIÓN

Yo, José Gonzalo Béjar Albán, 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.

Sr. José Gonzalo Béjar Albán

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por José Gonzalo Béjar Albán, bajo mi supervisión.

Ing. Xavier Calderón, M.Sc.
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Son innumerables los momentos que han sido parte del camino para culminar este trabajo. Ha sido una tarea larga que comenzó hace 5 años cuando entré por primera vez a las aulas de la facultad y hoy rinde sus primeros frutos con la consecución de este logro tan grande para mí. Muchas personas merecen mis agradecimientos, pero quiero comenzar agradeciendo a Dios y a la Madre Dolorosa quienes me han acompañado desde siempre, guiando mi camino y dándome aliento para continuar luego de cada tropiezo.

Agradezco de igual forma a mis padres y hermana por ser esa fuente discreta de confianza y seguridad que me ha ayudado a enfrentar todas las dificultades con esperanza risueña; esa esperanza que surge del apoyo incondicional de una familia entregada y amorosa, y que es capaz de volver invencible a todo hombre. Sin duda, a ellos les debo este logro, y todo lo que ahora soy.

Agradezco al Ing. Julio César Hidalgo, al Ing. José María Gómez de la Torre y al Ing. Fernando Santillán por toda su apertura y por permitir que este proyecto se lleve a cabo en la SUPERTEL; al Tnlg. Roberto Pérez y al Ing. Edwin Narváez por contribuir con sus ideas al proyecto; y finalmente a los funcionarios de la Dirección Nacional de Investigación Especial en Telecomunicaciones por todo su apoyo.

Agradezco también a mi director, Ing. Xavier Calderón, por entregar parte de su tiempo; y, con su experiencia, objetividad y exigencia, contribuir para crear un trabajo de calidad y excelencia, del cual me siento orgulloso. Agradezco de igual forma a cada uno de mis profesores durante mis años universitarios por ser parte importante en mi futuro profesional y contribuir a mi crecimiento personal.

Finalmente, agradezco a mis amigos por ser un gran apoyo y por compartir esta alegría tan grande junto a mí. Desearía nombrar a cada persona que ha contribuido directa o indirectamente en este logro, pero resultaría una lista interminable. Para todos ellos un inmenso GRACIAS y un abrazo desde el fondo de mi corazón.

José Béjar Albán

DEDICATORIA

Dedicado para Marcelo, Lucy y Ana Cristina, por su amor incondicional y entrega; por hacerme quien soy ahora y llenar de alegría mi corazón cada día;

Y para Juan Pablo, que pese a no estar más entre nosotros, vivirá por siempre en mi corazón y en mi memoria.

CONTENIDO

DECLARACIÓN ..... **I**
CERTIFICACIÓN ..... **II**
AGRADECIMIENTOS ..... **III**
DEDICATORIA ..... **IV**
CONTENIDO ..... **V**
ÍNDICE DE FIGURAS ..... **XI**
ÍNDICE DE TABLAS ..... **XV**
RESUMEN ..... **XVII**
PRESENTACIÓN ..... **XVIII**
CAPÍTULO 1: FUNDAMENTOS TEÓRICOS **1**
1.1 TELEFONÍA ANALÓGICA Y DIGITAL 1
1.1.1 Sistemas analógicos *1*
1.1.2 Sistemas digitales *4*
1.1.3 VoIP y Telefonía IP *4*
1.1.3.1 Telefonía IP 5
1.1.3.2 Voz sobre IP (VoIP) 7
1.1.3.2.1 Arquitectura VoIP 8
1.1.4 Protocolos VoIP *10*
1.1.4.1 *Session Initiation Protocol* (SIP) 10
1.1.4.1.1 Arquitectura SIP 10
1.1.4.1.2 Mensajes SIP 12
1.1.4.2 *Inter-Asterisk eXchange Protocol* (IAX) 13
1.1.4.2.1 Arquitectura IAX 13
1.1.4.2.2 Mensajes IAX 14
1.1.5 Protocolos para audio y video *16*
1.1.6 Códecs de audio *18*
1.1.7 Central telefónica *19*
1.2 PBX BASADAS EN SOFTWARE LIBRE 20
1.2.1 ASTERISK *20*
1.2.2 ELASTIX *22*
1.3 DIMENSIONAMIENTO TELEFÓNICO Y ENLACES 23
1.3.1 Intensidad de tráfico *23*
1.3.2 Modelos Erlang *24*

1.3.2.1 Erlang B 25
1.4 FRAUDE EN TELEFONÍA 26
1.4.1 Fraude por subscripción 27
1.4.2 Fraude interno 27
1.4.3 Fraude de roaming 28
1.4.4 Refilling 30
1.4.5 Robo de líneas 31
1.4.6 Fraude a PBX y Voicemail 32
1.5 SYSTEMAS TELEFÓNICOS "BYPASS" 33
1.5.1 Características de un "bypass" 35
1.5.2 Funcionamiento de un "bypass" 36
1.5.3 Tipos de "bypass" 40
1.5.3.1 Líneas convencionales y cuentas 40
1.5.3.2 Locutorios y líneas de cabinas públicas 40
1.5.3.3 Líneas celulares 40
1.5.4 Sistemas "bypass" con software libre 41
1.6 DISEÑO DE SOFTWARE 42
1.6.1 Programación orientada a objetos 43
1.6.1.1 Clase y Objeto 44
1.6.1.2 Herencia 44
1.6.1.3 Métodos 45
1.6.1.4 Mensajes 46
1.6.2 Programación orientada a componentes 46
1.6.3 Lenguaje UML 47
1.6.4 Programación Extrema 48
1.7 LENGUAJES DE PROGRAMACIÓN 49
1.7.1 Visual Studio 49
1.7.2 Java 50
1.7.3 PHP 51
1.7.4 Consideraciones de los lenguajes 52
CAPÍTULO 2: ANÁLSIS DE LA SITUACIÓN ACTUAL 53
2.1 TÉCNICAS PARA EL CONTROL DE "BYPASS" 53
2.1.1 Sistema de lazo cerrado o "loop" 56
2.1.1.1 SISLAC a través de tarjetas internacionales 58
2.1.1.2 SISLAC a través de portales web 59
2.1.2 Perfilamiento telefónico o profiling 60
2.1.3 Técnicas de ubicación de "bypass" 61
2.2. COMBATE A LOS "BYPASS" EN EL ECUADOR 63
2.2.1 Cantidad de "Bypass" intervenidos en los últimos años 64
2.2.2 Modalidades de operación de los "Bypass" en el Ecuador 67
2.2.3 Perjuicio económico 68
2.3 APLICACIÓN DEL SISTEMA DE LAZO CERRADO 70
2.3.1 Tráfico telefónico internacional en el Ecuador 70

2.3.2 Aplicación del sistema de lazo cerrado 74
2.4 MERCADO MUNDIAL DE LAS TELECOMUNICACIONES 77
2.4.1 Medidas de calidad 79
2.4.1.1 Tasa de tomas con respuesta (ASR) 79
2.4.1.2 Demora de respuesta después de la puerta de enlace (PGAD) 80
2.4.1.3 Duración media de la conversación (ALOC) 82
2.4.2 Particularidades del mercado 83
2.4.3 Compra y venta de minuntos en Internet 83
2.4.3.1 Arbinet 84
2.4.3.2 DirectInterconnect 86
2.4.3.3 Tseyva Ltd. y EXCILA Telecom 87
2.4.3.4 MinuteTraders 87
2.4.3.5 IPsmarx 88
2.4.3.6 2GoTEL 88
2.4.3.7 TerraSIP 88
2.4.3.8 VoIP.ms 89
2.4.3.9 Foros de compra y venta de minutos 89
2.5 EL ECUADOR Y LOS DELITOS EN TELECOMUNICACIONES 91

CAPÍTULO 3: DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA 93

3.1 REQUISITOS Y NECESIDADES DE LA SUPERINTENDENCIA 93
3.1.1 Requerimientos de la Superintendencia 93
3.1.2 Planteamiento de la solución 95
3.1.2.1 Análisis de una solución utilizando un grupo de módems telefónicos 97
3.1.2.2 Análisis de una solución utilizando una PBX ASTERISK o ELASTIX 98
3.1.2.3 Solución con módems vs PBX ASTERISK vs ELASTIX 99
3.1.2.4 Sistema gestor de llamadas ASTEM 101
3.1.3 Selección del software 103
3.1.4 Dimensionamiento de los elementos 103
3.2 DISEÑO DEL SISTEMA ASTEM 106
3.2.1 Casos de uso 106
3.2.1.1 Acceder al sistema 107
3.2.1.2 Salir del sistema 107
3.2.1.3 Realizar llamada de prueba 107
3.2.1.4 Programar llamadas de prueba 108
3.2.1.5 Generar alertas 108
3.2.1.6 Agregar tarjeta 109
3.2.1.7 Modificar tarjeta 109
3.2.1.8 Eliminar tarjeta 110
3.2.1.9 Consultar CDR’s de ASTERISK 110
3.2.1.10 Consultar los CDR's de ASTEM 111
3.2.1.11 Construir una búsqueda 111
3.2.1.12 Generar documentos en base a la información en las bases de datos 112
3.2.1.13 Generar datos estadísticos de las tarjetas utilizadas 112
3.2.1.14 Configurar del sistema ASTEM 112
3.2.1.15 Configurar ASTERISK 113

3.2.2 Diagrama de clases 113
3.2.2.1 Diagrama de clases de la aplicación servidor 113
3.2.2.2 Diagrama de clases de la aplicación cliente 115
3.2.3 Principales clases de la aplicación servidor ASTEM 116
3.2.3.1 Clase SrvOperadora 116
3.2.3.2 Clase SrvMonitor 119
3.2.3.3 Clase SrvCorreo 121
3.2.3.4 Clase SrvBaseDeDatos 123
3.2.3.5 Clase SrvConsola 125
3.2.3.6 Clase SrvRed 126
3.2.3.7 Clase SrvTarjeta 129
3.2.3.8 Clase SrvConfig 130
3.2.3.9 Clase SrvAsterisk 132
3.2.3.10 Clase SrvRegistros 132
3.2.3.11 Clase SrvAstem 133
3.2.4 Principales clases de la aplicación cliente ASTEM 136
3.2.4.1 Clase ClntTarjeta 136
3.2.4.2 Clase ClntConfig 136
3.2.4.3 Clase ClntAsterisk 137
3.2.4.4 Clase ClntRed 137
3.2.4.5 Clase ClntReportes 138
3.2.4.6 Clase ClntAstem 138
3.2.4.7 Clase ClntMenu 139
3.2.4.8 Ventanas y mensajes de la aplicación 139
3.2.5 Funcionamiento de la central telefónica ASTERISK 141
3.2.5.1 Plan de marcación 142
3.2.5.2 Configuración de troncales 142
3.2.5.3 Configuración de los usuarios 143
3.2.5.4 Configuración de CDRs 143
3.3 CONSIDERACIONES DE SEGURIDAD EN EL SISTEMA 144
3.3.1 Seguridad en la central ASTERISK 144
3.3.1.1 Seguridad en los canales 145
3.3.1.2 Seguridad en el plan de marcación 145
3.3.1.3 Seguridad física 146
3.3.2 Seguridad en la aplicación ASTEM 146
3.3.2.1 Proceso de autenticación de usuarios ASTEM 147
3.3.3 Seguridad en el sistema operativo 148
3.4 FORMATOS DE PRESENTACIÓN DE REPORTES 149
3.5 IMPLEMENTACIÓN DEL SISTEMA ASTEM 150
3.5.1 Particularidades durante el desarrollo 150
3.5.1.1 Organización de llamadas por troncales y número destino 151
3.5.1.2 Generación de llamadas por grupos 151
3.5.1.3 Envío de la configuración a través de la conexión 152
3.5.1.4 Envío de los datos de una consulta a la base de datos 152
3.5.1.5 Generación de reportes 152
3.5.1.6 Manejo de hilos en ASTEM 152

3.5.2 Consola de usuario del servidor ASTEM 153
3.5.2.1 Instrucción 'llamar' 153
3.5.2.2 Instrucción 'tarjeta' 154
3.5.2.3 Instrucción 'consulta' 154
3.5.2.4 Instrucción 'astem' 155
3.5.2.5 Instrucción 'asterisk' 156
3.5.2.6 Instrucción 'cronograma' 157
3.5.2.7 Instrucción 'estado' 158
3.5.2.8 Instrucción 'debug' 159
3.5.2.9 Instrucción 'quit' 159
3.5.2.10 Archivos de configuración del sistema 159
3.5.2.10.1 Estructura del archivo admin.astem 160
3.5.2.10.2 Estructura del archivo usuarios.astem 161
3.5.2.10.3 Estructura del archivo tarjeta.astem 161

CAPÍTULO 4: PRUEBAS DEL SISTEMA, BENEFICIOS Y LIMITACIONES 163

4.1 PRUEBAS REALIZADAS 163
4.1.1 Conexión entre la aplicación cliente y servidor 164
4.1.2 Administración de tarjetas de telefonía pre-pagada 168
4.1.3 Modificar las configuraciones del sistema ASTEM 173
4.1.4 Modificar las configuraciones de la PBX ASTERISK 177
4.1.5 Generar llamadas de prueba a un número de destino 180
4.1.6 Programar un grupo de llamadas de prueba 183
4.1.7 Identificar el campo de Caller ID en una llamada de lazo cerrado 188
4.1.8 Identificación de alertas y envío de notificaciones 191
4.1.9 Realizar una consulta a los CDR de ASTEM 194
4.1.10 Realizar una consulta a los CDR de ASTERISK 198
4.1.11 Datos estadísticos del sistema 200
4.1.12 Registros del sistema ASTEM 202
4.2 BENEFICIOS Y LIMITACIONES DEL SISTEMA 204
4.2.1 Beneficios económicos 204
4.2.2 Beneficios en tiempo 204
4.2.3 Beneficios funcionales 205
4.2.4 Limitaciones del sistema 206
4.3 COSTO ESTIMADO DEL SISTEMA 206
4.3.1 Costo de los equipos 206
4.3.2 Costo de diseño e implementación 207
4.3.3 Costo total 207
4.3.4 Comparación con aplicaciones comerciales similares 208
4.3.4.1 Comparación de ASTEM con SISPRIN 209
4.4 APLICACIONES ADICIONALES 211
4.5 EL FUTURO DEL SISTEMA ASTEM 211

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES 213

5.1 CONCLUSIONES 213

5.1.1 Conclusiones tecnológicas 213
5.1.2 Conclusiones económicas 217
5.1.3 Conclusiones funcionales 218
5.2 RECOMENDACIONES 219

GLOSARIO 222

BIBLIOGRAFÍA 228

ANEXOS 235

ÍNDICE DE ANEXOS

ANEXO A: GUÍA DE FUNCIONAMIENTO DEL SISTEMA

A. Interfaz gráfica y guía de funcionamiento del sistema
A.1. Conectar/Desconectar al servidor ASTEM
A.2. Realizar llamadas de prueba
A.3. Programar un grupo de llamadas de prueba
A.4. Administrar base de datos de tarjetas
A.5. Realizar una consulta a la base de datos
A.6. Generar reportes utilizando la información de una consulta
A.7. Realizar una consulta estadística de las tarjetas de telefonía pre-pagada
A.8. Configurar el sistema ASTEM
A.9. Modificar la configuración de la PBX ASTERISK

ANEXO B: ELEMENTOS EN UN DIAGRAMA DE ACTIVIDADES

B. Elementos en un diagrama de actividades

ANEXO C: ELEMENTOS DE UN DIAGRAMA DE CLASES

C. Elementos en un diagrama de clases
C.1. Clases
C.2. Relaciones

ANEXO D: PRUEBA DE CONSUMO DE RECURSOS DE ASTERISK

D. Prueba de consumo de recursos de ASTERISK

ANEXO E: PROFORMAS

ANEXO F: DOCUMENTOS

ÍNDICE DE FIGURAS

CAPÍTULO 1

FIGURA 1.1. ESTRUCTURA DE LA PSTN 2
FIGURA 1.2. PUERTOS FXS Y FXO EN EL LADO DEL ABONADO 3
FIGURA 1.3. INTERCONEXIÓN DE REDES DE TELEFONÍA TRADICIONAL, IP Y MÓVIL 5
FIGURA 1.4. DIFERENCIAS ENTRE SEÑALIZACIÓN TDM Y SIP 6
FIGURA 1.5. SISTEMA QUE UTILIZA VOIP 7
FIGURA 1.6. ELEMENTOS DE LA ARQUITECTURA VOIP 9
FIGURA 1.7. COMPONENTES DEL PROTOCOLO SIP 11
FIGURA 1.8. MENSAJES SIP EN EL ESTABLECIMIENTO DE UNA LLAMADA 12
FIGURA 1.9. MENSAJES IAX 15
FIGURA 1.10. EMPAQUETAMIENTO EN RTP 16
FIGURA 1.11. ESTRUCTURA DEL PROYECTO ELASTIX 22
FIGURA 1.12. MODELO DE TRÁFICO PARA ERLANG B 25
FIGURA 1.13. DIAGRAMA DE FRAUDE DE ROAMING 29
FIGURA 1.14. DIAGRAMA DE UN ENLACE UTILIZANDO REFILLING 30
FIGURA 1.15. DIAGRAMA DE UN FRAUDE A PBX 32
FIGURA 1.16. DIAGRAMA DE ELEMENTOS EN UN SISTEMA TELEFÓNICO "BYPASS" 34
FIGURA 1.17. DIAGRAMA DE UN "BYPASS" QUE PROCESA LLAMADAS ENTRANTES 35
FIGURA 1.18. DIAGRAMA DE UN "BYPASS" QUE PROCESA LLAMADAS SALIENTES 36
FIGURA 1.19. LLAMADA INTERNACIONAL A TRAVÉS DE UNA RUTA AUTORIZADA 37
FIGURA 1.20. LLAMADA INTERNACIONAL A TRAVÉS DE UNA RUTA NO AUTORIZADA 38
FIGURA 1.21. LLAMADA INTERNACIONAL A TRAVÉS DE UNA RUTA NO AUTORIZADA 39
FIGURA 1.22. REPRESENTACIÓN DE CLASES Y OBJETOS UML 44
FIGURA 1.23. REPRESENTACIÓN DE CLASES Y HERENCIAS EN UML 45
FIGURA 1.24. VISTA GENERAL DE LOS ELEMENTOS DEL LENGUAJE UML 47

CAPÍTULO 2

FIGURA 2.1. "BYPASS" SOBRE TELEFONÍA FIJA 54
FIGURA 2.2. "BYPASS" EN LÍNEAS DE TELEFONÍA MÓVIL 55
FIGURA 2.3. FUNCIONAMIENTO DE UN SISTEMA DE LAZO CERRADO O "LOOP" 56
FIGURA 2.4. TARJETA DE TELEFONÍA PRE-PAGADA DE LOS ESTADOS UNIDOS 58
FIGURA 2.5. LOGOS DE ALGUNOS PORTALES DE COMPRA Y VENTA DE MINUTOS 59
FIGURA 2.6. ESTRUCTURA DEL SISTEMA DE PERFILAMIENTO TELEFÓNICO 60
FIGURA 2.7. ESQUEMA DEL SISTEMA DE LOCALIZACIÓN POR MEDICIÓN DE TIEMPOS 62
FIGURA 2.8. NÚMERO TOTAL DE INTERVENCIONES REALIZADAS POR LA SUPERTEL EN LOS ÚLTIMOS 5 AÑOS 65
FIGURA 2.9. NÚMERO DE INTERVENCIONES REALIZADAS POR OPERADORA 66
FIGURA 2.10. MONTO DE LA PÉRDIDA EVITADA POR LA SUPERINTENDENCIA 69

FIGURA 2.11. CANTIDAD DE LLAMADAS INTERNACIONALES (2008 – 2010) 73
FIGURA 2.12. CANTIDAD DE MINUTOS DE TELEFONÍA INTERNACIONAL (2008 – 2010) ... 74
FIGURA 2.13. COMPORTAMIENTO DEL TRÁFICO TELEFÓNICO DURANTE EL AÑO 75
FIGURA 2.14. PRESENCIA DE ARBINET EN EL MUNDO 78
FIGURA 2.15. ESQUEMA REPRESENTATIVO DEL INTERVALO PGAD 81
FIGURA 2.16. VISTA DEL PORTAL DE NEGOCIACIÓN DE ARBINET 85
FIGURA 2.17. BÚSQUEDA DE COMPAÑÍAS EN DIRECTINTERCONECT.COM 86

CAPÍTULO 3

FIGURA 3.1. DIAGRAMA GENERAL DE LOS COMPONENTES DEL SISTEMA 96
FIGURA 3.2. GESTOR DE LLAMADAS UTILIZANDO MÓDEMS 97
FIGURA 3.3. GESTOR DE LLAMADAS UTILIZANDO ASTERISK 98
FIGURA 3.4. DIAGRAMA DEL SISTEMA GESTOR DE LLAMADAS ASTEM 102
FIGURA 3.5. DIAGRAMA DE LAS DOS ETAPAS EN UNA LLAMADA DE LAZO CERRADO 104
FIGURA 3.6. DIAGRAMA DE CASOS DE USO DEL SISTEMA 106
FIGURA 3.7. DIAGRAMA DE CLASES DE LA APLICACIÓN SERVIDOR 114
FIGURA 3.8. DIAGRAMA DE CLASES DE LA APLICACIÓN CLIENTE 115
FIGURA 3.9. DIAGRAMA DE ACTIVIDAD DE LA CLASE SRVOPERADORA 117
FIGURA 3.10. (A) DIAGRAMA DE ACTIVIDADES DE LA CREACIÓN DE ARCHIVOS DE LLAMADA. (B) DIAGRAMA DE ACTIVIDADES DE LA GENERACIÓN DE LLAMADAS 118
FIGURA 3.11. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVMONITOR* 120
FIGURA 3.12. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVCORREO* 122
FIGURA 3.13. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVBASEDEDATOS* 123
FIGURA 3.14. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVCONSOLA* 126
FIGURA 3.15. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVRED* 127
FIGURA 3.16. DIAGRAMA DE ACTIVIDADES DEL PROCESO DE AUTENTICACIÓN 128
FIGURA 3.17. DIAGRAMA DE ACTIVIDADES AL LEER LOS ARCHIVOS DE CONFIGURACIÓN 131
FIGURA 3.18. DIAGRAMA DE ACTIVIDADES DE LA CLASE *SRVREGISTROS* 132
FIGURA 3.19. DIAGRAMA DE ACTIVIDADES EN LA CLASE *SRVASTEM* 134
FIGURA 3.20. (A) DIAGRAMA DE ACTIVIDADES DEL PROCESADOR DE INSTRUCCIONES. (B) DIAGRAMA DE ACTIVIDADES DEL PROCESO DE RESPUESTA. 135
FIGURA 3.21. JERARQUÍA DE LOS OBJETOS GRÁFICOS DE LA APLICACIÓN CLIENTE 139
FIGURA 3.22. VENTANA DE CONFIGURACIÓN DE ASTEM 141
FIGURA 3.23. ESQUEMA DE AUTENTICACIÓN ASTEM 148
FIGURA 3.24. FORMATO DE REPORTES GENERADOS POR ASTEM 149
FIGURA 3.25. DIAGRAMA DE LA IMPLEMENTACIÓN DEL SISTEMA ASTEM 151
FIGURA 3.26. CONSOLA DE LA APLICACIÓN SERVIDOR ASTEM 153

CAPÍTULO 4

FIGURA 4.1. VENTANA DE INFORMACIÓN DEL SISTEMA 164
FIGURA 4.2. ARCHIVO DE CONFIGURACIÓN DE RED DEL EQUIPO SERVIDOR 165

FIGURA 4.3. CONFIGURACIÓN DE LOS PARÁMETROS DE RED EN EL EQUIPO CLIENTE ... 166
FIGURA 4.4. MENSAJE DE RESPUESTA DEL SERVIDOR CUANDO LA AUTENTICACIÓN FALLA ... 166
FIGURA 4.5. VENTANA DE AUTENTICACIÓN DE LA APLICACIÓN CLIENTE ... 167
FIGURA 4.6. MENSAJE DE AUTENTICACIÓN CONFIRMADA ... 167
FIGURA 4.7. VENTANA PRINCIPAL DEL SISTEMA ASTEM ... 167
FIGURA 4.8. OPCIÓN "DESCONECTAR" EN LA VENTANA PRINCIPAL DEL SISTEMA ... 168
FIGURA 4.9. MENSAJE DE FINALIZACIÓN DE LA CONEXIÓN CON EL SERVIDOR ... 168
FIGURA 4.10. BOTÓN DE LA VENTANA DE ADMINISTRACIÓN DE TARJETAS ... 169
FIGURA 4.11. VENTANA DEL ADMINISTRADOR DE TARJETAS DEL SISTEMA ... 169
FIGURA 4.12. MENSAJE DE ACTUALIZACIÓN DE LOS DATOS DE LA TARJETA ... 170
FIGURA 4.13. PRIMER MENSAJE DE INGRESO DE UNA NUEVA TARJETA ... 171
FIGURA 4.14. OPCIONES DE LA TARJETA ELIMINADA ... 171
FIGURA 4.15. MENSAJE DE CONFIRMACIÓN DE QUE LA TARJETA HA SIDO BORRADA ... 172
FIGURA 4.16. MENSAJE DE CIERRE DE LA VENTANA DE CONFIGURACIONES DEL SISTEMA ... 172
FIGURA 4.17. VENTANA DE SELECCIÓN DE UNA TARJETA MODELO ... 173
FIGURA 4.18. VENTANA DE INGRESO A LA CONFIGURACIÓN ASTEM ... 174
FIGURA 4.19. VENTANA DE CONFIGURACIONES DEL SISTEMA ... 174
FIGURA 4.20. OPCIONES MODIFICADAS EN LA PESTAÑA ASTEM ... 174
FIGURA 4.21. OPCIONES MODIFICADAS EN LA PESTAÑA OPERADORA ... 174
FIGURA 4.22. OPCIONES MODIFICADAS EN LA PESTAÑA MONITOR ... 175
FIGURA 4.23. OPCIONES MODIFICADAS EN LA PESTAÑA BASE DE DATOS ... 175
FIGURA 4.24. OPCIONES MODIFICADAS EN LA PESTAÑA CORREO PRINCIPAL ... 175
FIGURA 4.25. OPCIONES MODIFICADAS EN LA PESTAÑA CORREO SECUNDARIO ... 175
FIGURA 4.26. OPCIONES MODIFICADAS EN LA PESTAÑA USUARIO ... 176
FIGURA 4.27. OPCIONES MODIFICADAS EN LA PESTAÑA TRONCALES ... 176
FIGURA 4.28. OPCIONES MODIFICADAS EN LA PESTAÑA NÚMEROS ... 176
FIGURA 4.29. BOTONES DE LA VENTANA DE CONFIGURACIÓN DEL SISTEMA ... 176
FIGURA 4.30. VENTANA DE INGRESO A LA CONFIGURACIÓN ASTERISK ... 178
FIGURA 4.31. OPCIONES MODIFICADAS EN LA PESTAÑA PLAN DE MARCACIÓN ... 178
FIGURA 4.32. VENTANA DE CONFIGURACIÓN DE CANALES SIP ... 179
FIGURA 4.33. BOTONES DE ACCIÓN DE LA VENTANA DE CONFIGURACIONES DE ASTEM ... 179
FIGURA 4.34. MENÚ DE INGRESO A LA VENTANA DE GENERACIÓN DE LLAMADAS ... 181
FIGURA 4.35. OPCIONES DE GENERACIÓN DE LLAMADAS INDIVIDUALES ... 181
FIGURA 4.36. MENSAJE DE CONFIRMACIÓN DE LLAMADAS INICIADAS ... 181
FIGURA 4.37. EVENTOS DE INICIO DE LA SEGUNDA LLAMADA EN LA PBX ... 182
FIGURA 4.38. EVENTOS DE TERMINACIÓN DE LA SEGUNDA LLAMADA EN LA PBX ... 182
FIGURA 4.39. OPCIÓN "GENERAR PRUEBAS" ... 184
FIGURA 4.40. GENERADOR DE GRUPOS DE PRUEBAS DE LAZO CERRADO ... 184
FIGURA 4.41. CARPETAS CREADAS EN EL DIRECTORIO TEMPORAL DEL SISTEMA ... 185
FIGURA 4.42. INICIO DEL GRUPO DE PRUEBAS CON 2 LLAMADAS SIMULTÁNEAS ... 185

FIGURA 4.43. RECEPCIÓN DEL SEGUNDO PAR DE LLAMADAS DE PRUEBA..... 186
FIGURA 4.44. CONFIGURACIÓN DE FECHA Y HORA PARA LAS LLAMADAS DE PRUEBA.... 186
FIGURA 4.45. RECEPCIÓN DEL PAR DE LLAMADAS DE LAS PRUEBAS PROGRAMADAS.... 187
FIGURA 1.46. DIAGRAMA DE LOS EQUIPOS UTILIZADOS EN ESTE ESCENARIO 188
FIGURA 1.47. IMAGEN DEL CDR GENERADO POR EL ANALIZADOR DE PROTOCOLOS 189
FIGURA 1.48. IMAGEN DEL MENSAJE CAPTURADO POR EL ANALIZADOR DE PROTOCOLOS..... 190
FIGURA 4.49. IMAGEN DE ALERTAS ENVIADAS POR EL SISTEMA VÍA CORREO ELECTRÓNICO 192
FIGURA 4.50. CORREO ELECTRÓNICO GENERADO POR EL SISTEMA 193
FIGURA 4.51. INFORMACIÓN DE UNA CONSULTA "ESTÁNDAR" DEVUELTA POR EL SERVIDOR..... 195
FIGURA 4.52. VENTANA DE DEFINICIÓN DE CONSULTAS A LOS CDR'S DE ASTEM..... 195
FIGURA 4.53. INFORMACIÓN DEVUELTA POR EL SERVIDOR EN UNA CONSULTA PERSONALIZADA A LA BASE DE DATOS DE ASTEM..... 196
FIGURA 4.54. MENÚ DE GENERACIÓN DE REPORTES EN PDF Y HOJAS DE CÁLCULO.... 196
FIGURA 4.55. IMAGEN DE LAS OPCIONES DE REPORTE 197
FIGURA 4.56. PDF GENERADO POR EL SISTEMA EN BASE A LA INFORMACIÓN DE LA BASE DE DATOS DE CDR DE ASTEM..... 197
FIGURA 4.57. HOJA DE CÁLCULO GENERADA POR EL SISTEMA EN BASE A LA INFORMACIÓN DE LA BASE DE DATOS DE CDR DE ASTEM 197
FIGURA 4.58. VENTANA DE DEFINICIÓN DE CONSULTAS A LOS CDR'S DE ASTERISK. 199
FIGURA 4.59. SELECCIÓN DE PARÁMETROS GENERALES PARA LAS ESTADÍSTICAS 200
FIGURA 4.60. DATOS ESTADÍSTICOS DE TODAS LAS TARJETAS EN EL SISTEMA 201
FIGURA 4.61. DATOS ESTADÍSTICOS DE LAS TARJETAS "BESAME" EN EL SISTEMA 201
FIGURA 4.62. EVENTOS ALMACENADOS EN LOS LOGS DEL SISTEMA..... 203

ÍNDICE DE TABLAS

CAPÍTULO 1

TABLA 1.1. COMPARACIÓN ENTRE PROTOCOLOS IAX Y SIP 14
TABLA 1.2. COMPARACIÓN DE CÓDECS DE VOZ MÁS UTILIZADOS 19
TABLA 1.3. PERCEPCIÓN DE LOS USUARIOS SEGÚN EL GRADO DE SERVICIO O GOS 24

CAPÍTULO 2

TABLA 2.1. INTERVENCIONES A SISTEMAS DE TELEFONÍA TIPO "BYPASS" 64
TABLA 2.2. NÚMERO DE INTERVENCIONES REALIZADAS POR OPERADORA ENTRE EL 2005 AL 2010 65
TABLA 2.3. MONTO QUE LA SUPERTEL EVITÓ PERDER EN LOS ÚLTIMOS 5 AÑOS 69
TABLA 2.4. CANTIDAD DE LLAMADAS INTERNACIONALES DURANTE EL 2008 71
TABLA 2.5. CANTIDAD DE LLAMADAS INTERNACIONALES DURANTE EL 2009 72
TABLA 2.6. CANTIDAD DE LLAMADAS INTERNACIONALES DURANTE EL 2010 72
TABLA 2.7. CANTIDAD DE LLAMADAS ENTRANTES ANUALES 75

CAPÍTULO 3

TABLA 3.1. MATRIZ DE VALORACIÓN DE ALTERNATIVAS PARA EL GESTOR DE LLAMADAS 100
TABLA 3.2. MATRIZ DE DECISIÓN DE ALTERNATIVAS PARA EL GESTOR DE LLAMADAS ... 101
TABLA 3.3. COMPARACIÓN DE LOS LENGUAJES DE PROGRAMACIÓN 103
TABLA 3.4. RECOMENDACIÓN DE DIMENSIONAMIENTO DE PBX ASTERISK 105
TABLA 3.5. CASO DE USO "ACCEDER AL SISTEMA" 107
TABLA 3.6. CASO DE USO "SALIR DEL SISTEMA" 107
TABLA 3.7. CASO DE USO "REALIZAR LLAMADA DE PRUEBA" 108
TABLA 3.8. CASO DE USO "PROGRAMAR LLAMADAS DE PRUEBA" 108
TABLA 3.9. CASO DE USO "GENERAR ALERTAS" 109
TABLA 3.10. CASO DE USO "AGREGAR TARJETA" 109
TABLA 3.11. CASO DE USO "MODIFICAR TARJETA" 110
TABLA 3.12. CASO DE USO "ELIMINAR TARJETA" 110
TABLA 3.13. CASO DE USO "CONSULTAR CDR'S DE ASTERISK" 111
TABLA 3.14. CASO DE USO "CONSULTAR NOTIFICACIONES GENERADAS" 111
TABLA 3.15. CASO DE USO "CONSTRUIR BÚSQUEDA" 111
TABLA 3.16. CASO DE USO "GENERAR REPORTE DE REGISTROS" 112
TABLA 3.17. CASO DE USO "CONSULTAR ESTADO" 112
TABLA 3.18. CASO DE USO "CONFIGURACIÓN DEL SISTEMA ASTEM" 113
TABLA 3.19. CASO DE USO "CONFIGURAR ASTERISK" 113
TABLA 3.20. OPCIONES DE CONFIGURACIÓN DEL ARCHIVO "ADMIN.ASTEM". 161

CAPÍTULO 4

TABLA 4.1 LISTA DE EQUIPOS Y SU VALOR APROXIMADO EN EL MERCADO..... 206
TABLA 4.2 COSTOS DE DISEÑO E IMPLEMENTACIÓN..... 207
TABLA 4.3 COSTO FINAL DEL DESARROLLO DEL SISTEMA Y EQUIPOS..... 207
TABLA 4.4. COSTOS ADICIONALES EN LA OFERTA DEL SISTEMA. 208
TABLA 4.5 COSTO FINAL DE UNA PROPUESTA DEL SISTEMA..... 208
TABLA 4.6. CARACTERÍSTICAS DE LOS SISTEMAS SISPRIN Y ASTEM 210
TABLA 4.7. COSTOS DE IMPLEMENTACIÓN DE LOS SISTEMAS ASTEM Y SISPRIN..... 210

RESUMEN

En el primer capítulo, el presente trabajo recoge los aspectos generales de telefonía y las tecnologías que han sido utilizadas en los últimos años. Esto incluye las características de VoIP y su aplicación en soluciones telefónicas basadas en IP. De igual forma se menciona características de centrales telefónicas con software libre, las cuales se han vuelto bastante populares.

En el primer capítulo también se realiza una revisión sobre metodologías de diseño de software y lenguajes de programación, los cuales serán las herramientas utilizadas en el desarrollo del sistema propuesto. Se incluye también una revisión de los principales tipos de delitos en telecomunicaciones con énfasis en los sistemas telefónicos “bypass”; se revisa sus métodos de operación y técnicas para combatirlos.

En el segundo capítulo se realiza un análisis de la situación actual del Ecuador respecto a los sistemas “bypass” en los últimos años, considerando los montos aproximados de pérdida evitada por este tipo de delitos.

En el tercer capítulo se diseña una aplicación distribuida basada en una técnica de combate a los sistemas “bypass” denominada “prueba de lazo cerrado”. Esta aplicación utiliza una central telefónica basada en software libre para realizar llamadas de lazo cerrado y analiza los resultados obtenidos automatizando el proceso. El sistema está compuesto por una central telefónica ASTERISK, una base de datos en MySQL y la aplicación desarrollada en este proyecto. Luego del diseño e implementación del sistema, se detallan los aspectos más importantes del funcionamiento del mismo.

En el capítulo cuarto se realizan pruebas de funcionamiento del sistema y una comparación con soluciones similares. Luego se listan las ventajas del desarrollo realizado, costos de desarrollo e implementación y sus posibles aplicaciones adicionales. Finalmente, en el capítulo quinto, se listan las conclusiones y recomendaciones alcanzadas durante el desarrollo de este proyecto.

PRESENTACIÓN

El sector de las telecomunicaciones ha evolucionado radicalmente en los últimos años y junto con estos cambios han aparecido nuevos métodos de fraude tecnológico. El presente trabajo recoge las principales características de estos tipos de delitos, comenzando por las tecnologías de telefonía más utilizadas en la actualidad.

El Ecuador se encuentra en un proceso de transición adaptándose aún a nuevas tecnologías de comunicación. Esto conlleva la necesidad de considerar aspectos de seguridad, ya que un mundo de comunicaciones virtual ofrece tanto ventajas como vulnerabilidades. Es necesario entonces, entender las limitaciones tecnológicas y llevar nuestra imaginación un paso más adelante en busca de esos detalles que pueden perjudicar a usuarios y empresas.

En este sentido, el mercado de las telecomunicaciones en todo el mundo se encuentra cambiando radicalmente y tecnologías como VoIP han revolucionado la manera de entender la telefonía. Por esto, los delitos en el Ecuador han migrado hacia nuevas técnicas, lo cual al mismo tiempo exige a los involucrados nuevas herramientas para combatirlas; herramientas acordes a la tecnología en el mundo.

La Superintendencia de Telecomunicaciones, en su riguroso combate a los delitos en telecomunicaciones en el Ecuador, a través de la Dirección Nacional de Investigación Especial en Telecomunicaciones, ha impulsado el desarrollo de un sistema que permite combatir los fraudes telefónicos denominados sistemas “bypass”. Dicho sistema ofrece un nuevo enfoque tecnológico y abre un campo de posibilidades futuras a fin de aprovechar y desarrollar nuevas tecnologías.

Cabe destacar que siendo el primer éxito en un camino de retos e innovaciones tecnológicas, el desarrollo de este sistema, denominado ASTEM, es una pequeña muestra del potencial que nuestras ideas, concebidas en la mitad del mundo, pueden llegar a tener.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 TELEFONÍA ANALÓGICA Y DIGITAL [12], [22], [31], [49], [59], [70]

1.1.1 SISTEMAS ANALÓGICOS

En sus inicios, la telefonía como un sistema pionero en los servicios de telecomunicaciones, surge para facilitar la comunicación entre personas a largas distancias. En la actualidad, se vive en una sociedad de la información en la cual la telefonía ha afianzado su carácter móvil y se ha convertido en un servicio indispensable.

La telefonía nació como un sistema analógico de comunicación entre personas, creado para la transmisión de voz humana en tiempo real a través de una red

conocida como Red Telefónica Pública Conmutada o PSTN[1] por sus siglas en inglés (*Public Switched Telephone Network*). La PSTN es una red de telecomunicaciones conmutada ya que cuando se realiza una llamada, la marcación de un número cierra un conmutador y establece así un circuito con el receptor de la llamada. Dicho circuito es dedicado a una sola comunicación y dura el tiempo que la llamada se encuentre activa.

Cada línea en una PSTN tiene asignada una numeración específica (número telefónico) y está físicamente construida por dos hilos metálicos (conocidos como par de cobre), que se extienden desde la central telefónica hasta la instalación del abonado (se conoce también como bucle de abonado). Cada central administra las líneas de abonado de un área geográfica determinada. A su vez, las centrales telefónicas están conectadas entre sí con otro tipo de enlaces que pueden manejar una gran cantidad de canales simultáneos. En el Ecuador la PSTN es digital casi en su totalidad, salvo el bucle de abonado que aún es analógico.

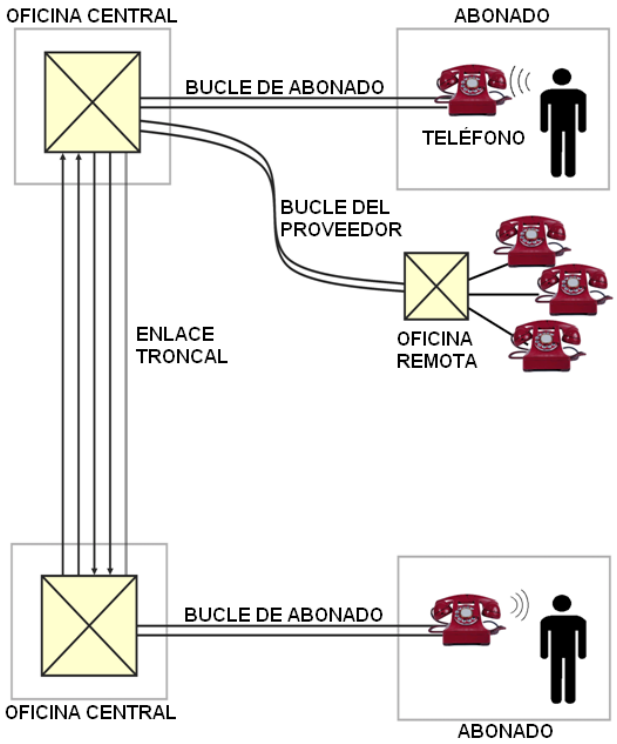


Figura 1.1. Estructura de la PSTN [59]

La PSTN está formada por 4 componentes básicos [59]:

[1] PSTN también es conocida como Red Telefónica Conmutada (RTC) o Red Telefónica Básica (RTB).

- Oficina Central.- Contiene el *switch* que se encarga de conmutar las llamadas y establecer los circuitos.

- Teléfono.- Equipo terminal en el lado del usuario.

- Bucle local.- Un par de cobre que conecta un teléfono al *switch* ubicado en la Oficina Central y representa un circuito dedicado para ese teléfono.

- Enlaces troncales.- Conectan 2 o más oficinas centrales y permite la conmutación entre diferentes *switch*.

En la Figura 1.1 se muestra un esquema de los componentes de la PSTN.

Figura 1.2. Puertos FXS y FXO en el lado del abonado [49]

El sistema utiliza señalización por tonos para identificar equipos y realizar llamadas. Esta señalización es dada por la central telefónica a través del bucle local, por lo que se pueden identificar dos tipos de interfaces en la red, como se observa en la Figura 1.2: [59]

- Oficina de Central Telefónica Externa, o FXO por sus siglas en inglés (*Foreign Exchange Office*).- Es el puerto por el cual un abonado recibe una línea telefónica. Los puertos FXO tienen la funcionalidad de enviar señales de descolgado o colgado conocido como cierre de bucle. Este puerto se encuentra en los dispositivos telefónicos como teléfono o fax.

- Abonado de la Central Telefónica Externa, o FXS por sus siglas en inglés (*Foreign Exchange Subscriber*).- Es el puerto por el cual el abonado se conecta a una línea telefónica, ya sea de la PSTN o de la central de la empresa. En otras palabras, la interfaz FXS provee el servicio al usuario final (teléfonos, módems o faxes). Los puertos FXS son los encargados de:

- Proporcionar tono de marcado.
- Suministrar tensión (y corriente) al dispositivo final.

1.1.2 SISTEMAS DIGITALES

Los sistemas digitales son una modernización de los métodos de comunicación analógicos que integran conceptos de modulación y codificación. Modulación es el proceso por el cual una señal analógica de baja frecuencia es transportada utilizando una señal con frecuencia más alta (portadora) en la que pueda ser transmitida más fácilmente. [18], [22]

La Codificación de una señal es un proceso de digitalización, es decir, es una técnica donde se asigna un código binario a cada nivel de una señal analógica que ha sido discretizada a fin de transmitir únicamente dicho código e interpretarlo en el lado del receptor para recuperar la señal analógica. [18], [22]

Si bien estos procesos implican la pérdida de cierta cantidad de información en la señal transmitida, permite a su vez aprovechar las ventajas de los sistemas digitales para la transmisión de información. Entre las principales mejorías destaca la resistencia al ruido y menor atenuación.

En los sistemas telefónicos actuales es común encontrar funcionando tanto sistemas analógicos como digitales. Los primeros se utilizan para proveer el servicio telefónico al usuario final a través del bucle local mientras que los segundos realizan la interconexión entre centrales telefónicas a través de enlaces troncales.

1.1.3 VOIP Y TELEFONÍA IP

Es muy común el descuido con que se usan los términos de “Telefonía IP” y “VoIP”, al punto en que ciertos autores los presentan como sinónimos. Figurativamente, VoIP se asemeja a rieles de tren innovadoras, mientras que Telefonía IP refiere a todos los usos que se le puede dar a esos rieles de tren, no solo con trenes de pasajeros sino con todo tipo de trenes, auto ferros y cargas que las puedan aprovechar.

Voz sobre IP (VoIP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La telefonía IP es mucho más que solo VoIP; es integrar servicios que tradicionalmente se ofrecían en PBX con la ubicuidad de Internet (redes IP). [44]

1.1.3.1 Telefonía IP

La Telefonía IP es una evolución tecnológica de la telefonía tradicional. En este nuevo concepto, los servicios ofrecidos por la telefonía tradicional sumados a otros servicios adicionales son ofrecidos a través de redes IP. Los mensajes de voz y datos se transportan utilizando paquetes IP a través de una red de datos, permitiendo ofrecer servicios como voz, fax, mensajes de voz, etc.

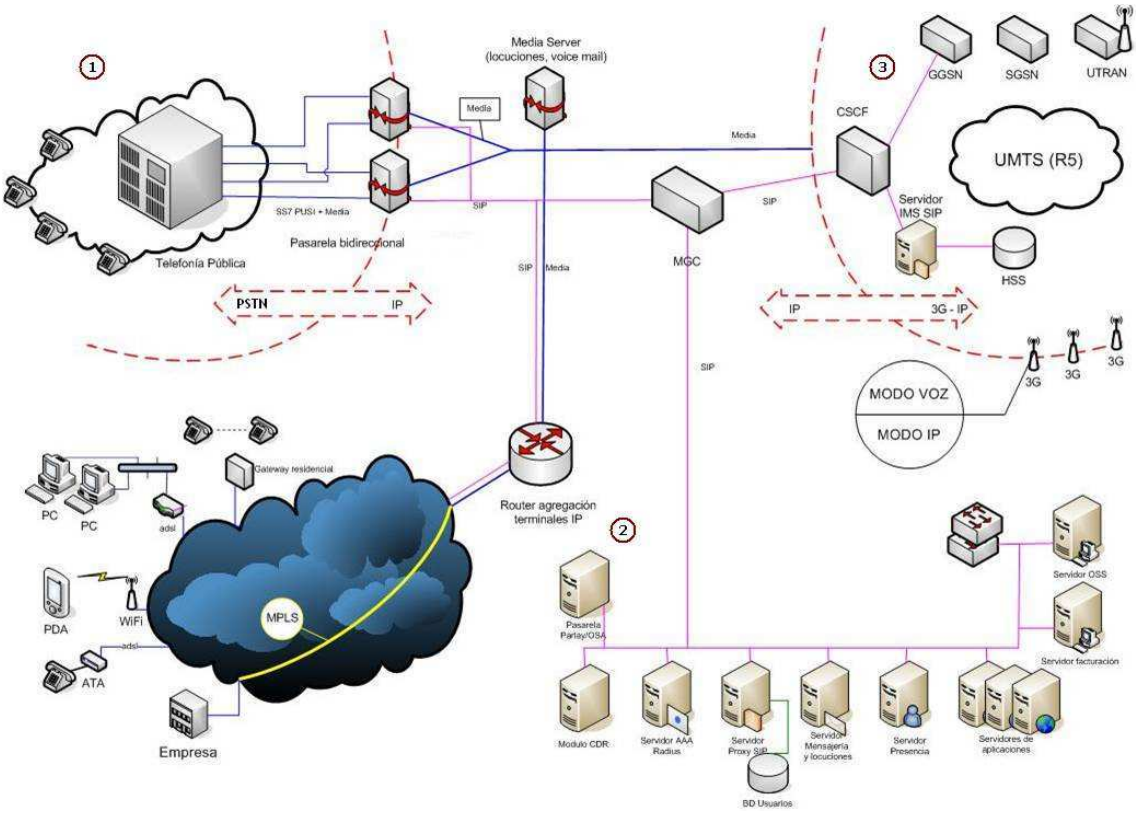


Figura 1.3. Interconexión de redes de telefonía tradicional, IP y móvil [74]

La Telefonía IP es considerada por varios autores como una aplicación de VoIP. Esta tecnología brinda nuevos servicios a los usuarios y una serie de beneficios económicos y tecnológicos como [67]:

- Interoperabilidad con redes telefónicas tradicionales.
- Calidad de servicio. El concepto de calidad incluye:

a. Redes de alta disponibilidad.
b. Calidad de voz.

- Servicios de valor agregado.

La conexión entre redes de telefonía heterogéneas (tradicional, IP y móvil) se realiza a través de equipos específicos que permiten la comunicación entre los diferentes protocolos. Como se puede observar en la Figura 1.3, equipos Gateway son utilizados con este fin.

En la parte superior izquierda de la Figura 1.3, en el punto 1, se observa una red telefónica tradicional; en la mitad inferior de la figura, en el punto 2, se muestra un diagrama de una red de Telefonía IP; por último, en la esquina superior derecha, o punto 3, se observa el diagrama de una red de telefonía móvil.

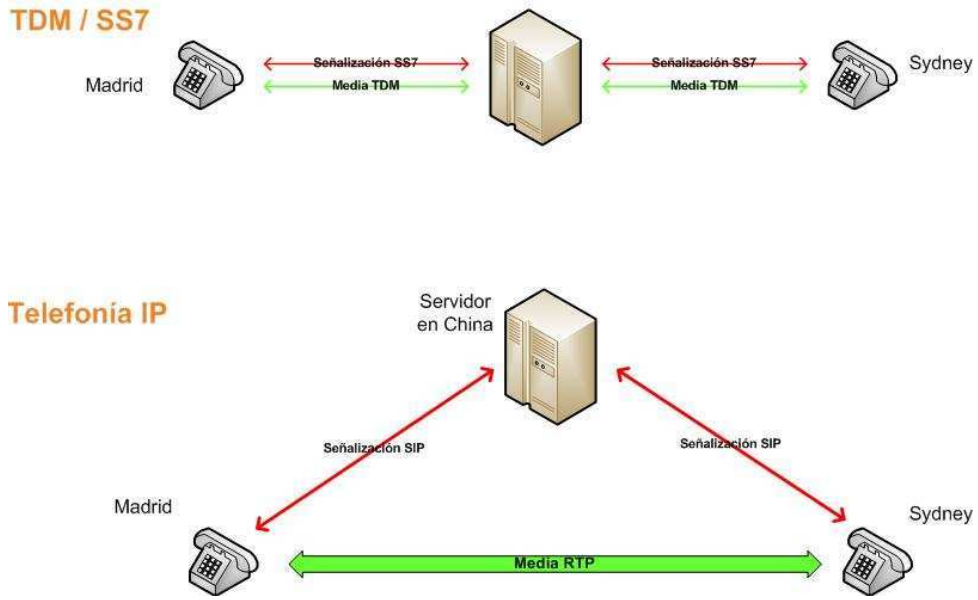


Figura 1.4. Diferencias entre señalización TDM y SIP [74]

En la Telefonía IP se destacan ciertas diferencias en cuanto al proceso de una llamada telefónica. En la telefonía convencional se utiliza TDM[2] para voz y SS7[3] para señalización; aquí, la información de los usuarios es centralizada, y la señalización puede utilizar las mismas redes (canal asociado) o redes diferentes (canal no asociado). Por otro lado, en telefonía IP, se utiliza señalización SIP[4], la

[2] Técnica en la cual se transmiten varias señales por un mismo canal.
[3] Tipo de señalización que permite el establecimiento y finalización de llamadas.
[4] Protocolo creado para la iniciación, modificación y finalización de sesiones multimedia.

cual viaja hacia los terminales a través de la central, y la voz, transportada por RTP[5], se transmite directamente. Véase la Figura 1.4.

La Telefonía IP por ser descentralizada permite tener movilidad a los terminales y al servidor. Es decir, el servidor puede estar en un país mientras los terminales en otro, y de igual forma, éstos pueden cambiar su ubicación sin necesidad de cambiar de número. Esto abre la puerta a un reto regulatorio, ya que esta tecnología permite conectar redes telefónicas de diferentes países utilizando un único sistema presente en ambos países; el reto se concentra en definir qué leyes regulan la operación del sistema [74].

1.1.3.2 Voz sobre IP (VoIP)

El protocolo de *Voz sobre IP* o VoIP[6] es una tecnología que permite la transmisión de voz utilizando paquetes en una red IP. Utilizando VoIP es posible realizar llamadas telefónicas a través de una red IP como Internet. Las llamadas pueden ser generadas desde un computador o un número telefónico, como se observa en la Figura 1.5. [39], [53]

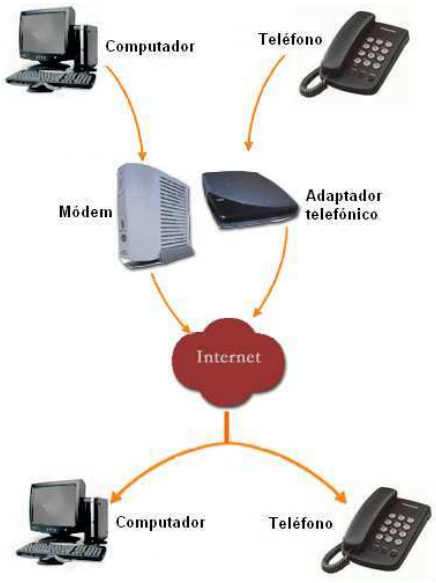


Figura 1.5. Sistema que utiliza VoIP [39]

La tecnología VoIP utilizada en Telefonía IP permite realizar llamadas dentro de la misma red y hacia la red de telefónica pública conmutada. Algunos proveedores

[5] Protocolo utilizado para la transmisión de información en tiempo real, como audio y vídeo.
[6] VoIP por sus siglas en inglés *Voice Over Internet Protocol*.

permiten realizar llamadas únicamente a los elementos de la red, sin embargo, es posible realizar llamadas hacia otras redes que se encuentren conectadas.

Este tipo de tecnología funciona principalmente sobre computadores con software que permiten realizar llamadas VoIP, o un teléfono VoIP. Sin embargo, existen dispositivos que permiten utilizar un teléfono analógico con VoIP [53].

El *Grupo Europeo de Regulación para las Comunicaciones Electrónica*s, BEREC[7], clasifica los servicios de tráfico de VoIP de la siguiente forma [35]:

1. *Voz sin números geográficos*.- Este tipo de servicio no permite el acceso a la red de telefonía pública conmutada.

2. *Salida de voz*.- Permite realizar llamadas hacia la red de telefonía pública conmutada, pero no recibe llamadas. El abonado no dispone de un número telefónico E.164[8].

3. *Entrada de voz*.- Permite recibir llamadas desde la red telefónica pública conmutada, pero no permite realizar llamadas. Para esto, el abonado cuenta con un número telefónico E.164.

4. *Telefonía de voz*.- Estos servicios de voz permiten realizar y recibir llamadas hacia y desde la red telefónica pública conmutada. Para esto se dispone de un número telefónico E.164.

Durante los últimos años ha crecido la utilización de VoIP a través de Internet con software como Skype, Google Talk, etc. En algunos casos, como Skype, utilizan protocolos propietarios desarrollados para optimizar el consumo de ancho de banda, haciendo posible una conversación de buena calidad utilizando una conexión a Internet compartida. [3]

1.1.3.2.1 Arquitectura VoIP

Una característica muy particular de VoIP es su arquitectura; VoIP puede ser implementado con una arquitectura centralizada o distribuida. La arquitectura

[7] Acrónimo de sus siglas en inglés *Body of European Regulators for Electronic Communications*, antes *European Regulators Group* o ERG.
[8] E.164 es el nombre de la recomendación de la Unión Internacional de Telecomunicaciones (UIT) que define el plan de numeración telefónica internacional.

distribuida ofrece mayores beneficios que la arquitectura centralizada, aunque esta primera es más compleja. [49]

La arquitectura centralizada es sencilla de implementar, aunque conlleva el riesgo de no disponer de los servicios si el servidor falla, o de limitar futuras expansiones de la red. [49]

Muchos de los protocolos utilizados en VoIP han sido estandarizados por la UIT.

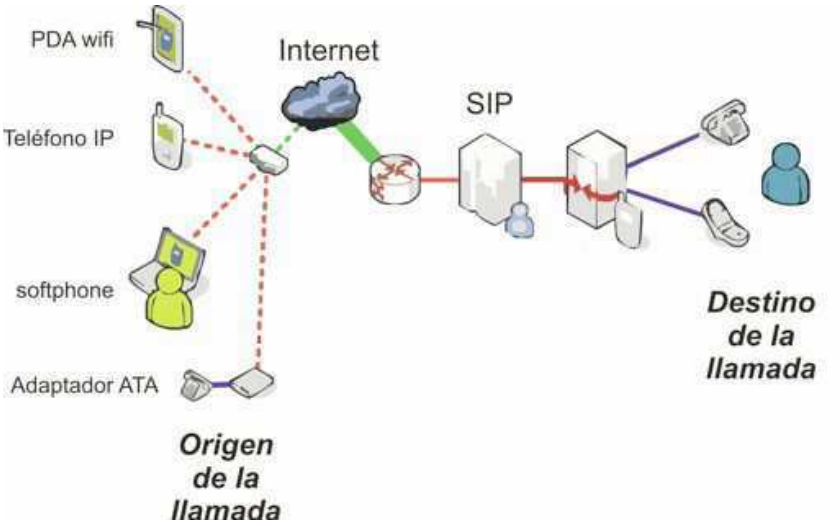


Figura 1.6. Elementos de la arquitectura VoIP [49]

En la Figura 1.6 se muestra un diagrama de los elementos en una arquitectura VoIP general, donde se puede destacar los siguientes dispositivos: [49]

- Central IP.- Es la central telefónica o PBX que encargada de controlar las llamadas en la red.
- Teléfono IP.- Es un teléfono similar a los utilizados tradicionalmente, pero con la particularidad de manejar VoIP.
- Softphone.- Es un software instalado sobre un computador que realiza las funciones de Teléfono IP.
- Adaptador ATA.- Es un dispositivo que permite conectar un teléfono analógico a una red IP.
- H.323/SIP.- Son los protocolos utilizados en la red para comunicar los dispositivos y gestionar las llamadas de VoIP.
- B2BUA (Agente de usuario o *Back-to-Back User Agent*).- Es una entidad lógica encargada de administrar las llamadas.

1.1.4 PROTOCOLOS VOIP

1.1.4.1 *Session Initiation Protocol* (SIP)

El Protocolo de Inicialización de Sesión, o SIP por sus siglas en inglés (*Session Initiation Protocol*), fue desarrollado por la IETF en el RFC 2543, conocido hoy en día como SIPv1. En el 2002, la IETF[9] lanza la versión de SIP que hasta hoy prevalece en el RFC 3261. SIP es un protocolo que define los parámetros de señalización para iniciar, modificar y terminar a aplicaciones de mensajería instantánea, de video, de audio, conferencias y aplicaciones similares, conocidas como sesiones multimedia. Textualmente el RFC 3261 define su funcionamiento de la siguiente forma: [57], [50]

> "SIP es un protocolo de control de la capa de aplicación que puede establecer, modificar, y terminar sesiones multimedia como llamadas telefónicas por Internet. SIP puede también invitar participantes a sesiones existentes, como conferencias."[10]

1.1.4.1.1 Arquitectura SIP

SIP contiene una serie de características que lo hacen muy útil para la gestión de sesiones multimedia, es decir transporte de voz, video y muchos servicios más. De las funciones de señalización de SIP, se pueden mencionar: [65]

- Establecer, modificar y finalizar llamadas.
- Registrar y localizar participantes.
- Gestión del conjunto de participantes y de los componentes del sistema.
- Descripción de características de las sesiones y negociación de capacidades de los participantes.

En cuanto a su arquitectura, SIP es un protocolo cliente – servidor que utiliza mensajes de petición y respuesta para gestionar las sesiones multimedia. En

[9] Acrónimo del Grupo de Trabajo de Ingeniería de Internet, o *Internet Engineering Task Force*.
[10] Documento RFC3261, http://tools.ietf.org/html/rfc3261

relación a otros protocolos, SIP es sencillo de implementar y utiliza conceptos de otros servicios como WEB, DNS, etc. [70]

Los elementos de red del protocolo SIP son aquellos encargados de cumplir las funciones del protocolo. Estos elementos interactúan entre los componentes cuando se lleva a cabo una llamada. En la Figura 1.7 se muestra un diagrama de algunos componentes del protocolo SIP, estos son: [65], [70], [57]

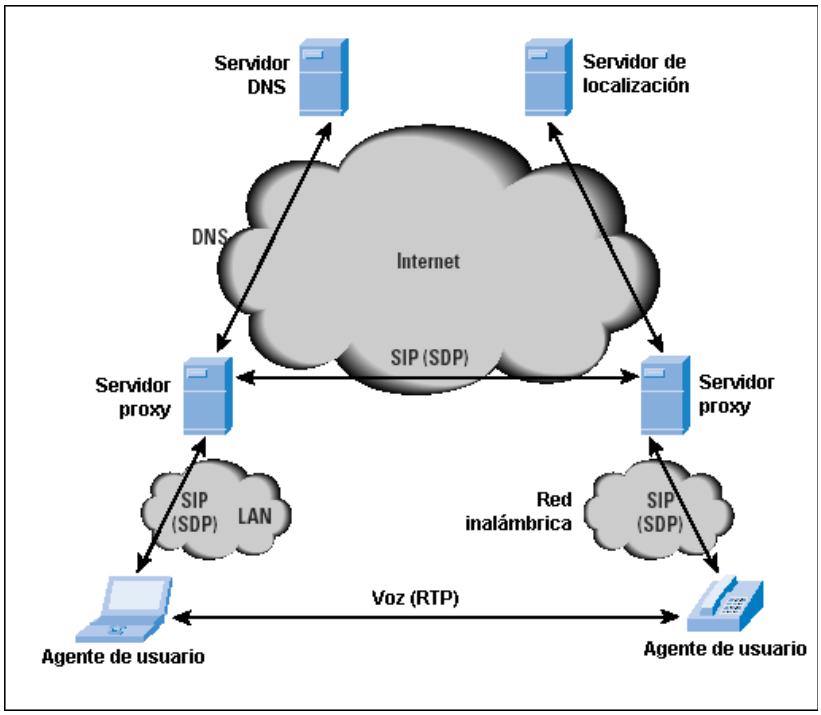


Figura 1.7. Componentes del protocolo SIP [57]

- Agente de usuario.- El agente de usuario reside en cada componente SIP y actúa de dos formas,
    - Agentes de Usuario Cliente (UAC): Genera peticiones SIP.
    - Agentes de Usuario Servidor (UAS): Recibe peticiones SIP y genera respuestas que acepten, rechacen o redirijan la petición.
- Servidor de Redirección.- El servidor de redirección es usado durante el establecimiento de una sesión para determinar la dirección del destinatario. Para la redirección, el servidor envía esta información al dispositivo llamante, dirigido al UAC.

- Servidor Proxy.- El servidor proxy es un elemento intermediario que actúa como cliente y servidor con el fin de realizar peticiones en nombre de otros clientes. Un servidor proxy primario cumple funciones de enrutamiento, es decir, que se asegura que una solicitud sea enviada al elemento más cercano a su destino, de ser necesario. Los servidores proxy también son útiles para la aplicación de políticas (por ejemplo, asegurar que un usuario está autorizado a realizar llamadas). Un proxy interpreta, y si es necesario, reescribe partes de una solicitud antes de reenviarla.

- Servidor de registro.- Un servidor de registro es aquel que acepta peticiones de registro, y coloca la información que recibe (dirección IP y SIP asociadas al dispositivo) en el servidor de localización.

- Servidor de localización: El servidor de localización es usado por el redirector o el proxy para obtener información acerca de la posible localización de los destinatarios. El servidor de localización mantiene una base de los dispositivos y sus direcciones SIP e IP.

Otra característica importante de SIP es que se integra fácilmente con otros protocolos como RVSP[11], RTP o RTSP[12]. Gracias al protocolo SDP se puede formar una completa arquitectura multimedia. SIP[13] utiliza estos protocolos para llevar a cabo el intercambio de paquetes de voz en una llamada. [57]

1.1.4.1.2 Mensajes SIP

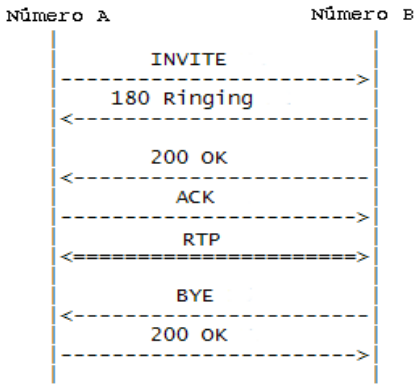


Figura 1.8. Mensajes SIP en el establecimiento de una llamada [71]

[11] Es un protocolo de red que permite al receptor solicitar calidad de servicio en la transmisión.
[12] Protocolo que establece y controla flujos sincronizados de datos de audio o de video.
[13] Protocolo para describir los parámetros de inicialización de los flujos multimedia.

En la Figura 1.8 se pueden observar los mensajes SIP que intervienen en el proceso de una llamada. SIP define 6 diferentes tipo de mensajes para las peticiones de los clientes: [70]

- INVITE: Inicia el establecimiento de una sesión con un usuario o servicio.
- ACK: Confirma un mensaje o el establecimiento de una sesión.
- OPTION: Solicita información sobre la capacidad de un servidor.
- BYE: Finaliza una sesión.
- CANCEL: Cancela una petición pendiente.
- REGISTER: Registra el agente de usuario.

Como se observa en la Figura 1.8, en una llamada exitosa intervienen los mensajes de INVITE, RINGING, OK, BYE y ACK. Las flechas que indican RTP representan el intercambio de mensajes de voz. [70]

1.1.4.2 *Inter-Asterisk eXchange Protocol* (IAX)

El Protocolo de Intercambio entre ASTERISK, o IAX por sus siglas en Inglés (*Inter-Asterisk eXchange Protocol*), fue desarrollado con el fin de implementar un protocolo que consuma poco ancho de banda, para conectar centrales telefónicas ASTERISK. Con el paso del tiempo, este protocolo ha sido utilizado también con dispositivos clientes y otros equipos, y no exclusivamente con servidores ASTERISK. En la actualidad se encuentra vigente la segunda versión de este protocolo, IAX2; sin embargo, ya que esta versión reemplazó a su predecesora, se la refiere comúnmente como IAX. [70],[31]

1.1.4.2.1 Arquitectura IAX

IAX trabaja sobre redes IP y fue diseñado originalmente para controlar y transmitir voz, sin embargo, sus características permiten que transmita video o voz. Los principales objetivos de IAX son: [31]

- Reducir el ancho de banda necesario para transmitir mensajes de voz o video, en especial voz.- La principal característica de IAX es ser un

protocolo binario. A diferencia de SIP, IAX transmite sus mensajes en binario lo cual implica un menor consumo de ancho de banda.

- Compatibilidad con el protocolo NAT.- Para trabajar adecuadamente con este servicio, IAX2 utiliza mensajes UDP sobre el puerto 4569, a diferencia de IAX que lo hacía en el puerto 5036. Además, la información de señalización y datos viajan juntas, lo que le da mayor facilidad para pasar por routers, firewalls y otros equipos de red.

Aunque IAX fue diseñado pensando en aplicaciones telefónicas, en su última versión permite trabajar con una gran cantidad de códecs, lo que le permite aumentar su funcionalidad dando soporte a otro tipo de aplicaciones. Esta característica lo convierte en una buena alternativa frente a SIP.

En la Tabla 1.1 se puede observar una comparación entre características mencionadas de los protocolos IAX y SIP.

	SIP	IAX	Comentario
Tipos de mensajes	Formato texto	Formato binario	IAX reduce el ancho de banda
Señalización	Datos y señalización en puertos distintos	Datos y señalización por el mismo puerto	SIP suele tener problemas con NAT
	El audio se transmite sin pasar por el servidor SIP	El audio pasa obligatoriamente por el servidor IAX	Mayor consumo de recursos en el servidor IAX
Estándar	IETF	En proceso	SIP es soportado por la mayoría de equipos.
Uso de puertos	1 señalización + 2 de voz o RTP (uno por sentido)	1 puerto para señalización y audio	SIP requiere de más puertos libres

Tabla 1.1. Comparación entre protocolos IAX y SIP [70], [31]

1.1.4.2.2 Mensajes IAX

IAX define dos tipos de tramas, en lugar de mensajes. A diferencia de otros protocolos, los mensajes están basados en estas tramas: [70], [31]

- Trama pequeña M o *Mini-frame*.- Esta trama es utilizada para enviar voz o video con una cabecera corta. Estas tramas no necesitan confirmación del lado del receptor y permiten enviar mayor cantidad de datos. Estos mensajes contienen una cabecera de 4 bytes.

- Trama completa F o *Full-frame*.- Esta trama es utilizada para enviar señalización, audio o video de forma confiable. Esta trama siempre debe ser respondida con un ACK para confirmar su recepción.

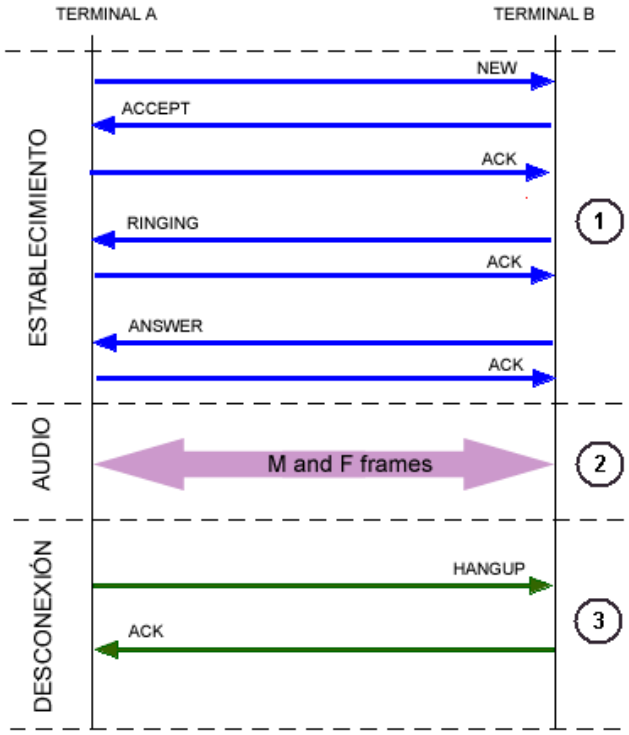


Figura 1.9. Mensajes IAX [70]

En la Figura 1.9 se muestra un diagrama del flujo de mensajes en una llamada IAX. Como se observa en la Figura, una llamada IAX tiene tres fases: [70]

1. *Establecimiento de la llamada*.- El establecimiento de la llamada inicia con un mensaje de señalización llamada *NEW* enviado desde el cliente que inicia la llamada. Luego del mensaje *NEW*, el cliente destino envía los mensajes *ACCEPT*, *RINGING* y *ANSWER*, que corresponden a los diferentes estados del cliente destino hasta contestar la llamada.

2. *Flujo de datos o flujo de audio*.- En esta fase se transmiten tramas F o M que contienen los mensajes de voz de la llamada telefónica.

3. *Liberación de la llamada o desconexión*.- Esta es la última fase de una llamada. La llamada concluye con un mensaje *HANGUP* enviado desde uno de los clientes que indica el fin de la llamada. El otro cliente responde a este mensaje con una confirmación de recibido o mensaje *ACK*.

1.1.5 PROTOCOLOS PARA AUDIO Y VIDEO

La aparición de diferentes medios de comunicación a través de la red, como Internet, telefonía sobre IP, videoconferencia, música y video bajo demanda, etc., creó la necesidad de definir un protocolo estándar que permita el transporte en tiempo real de esta información. Partiendo de esta necesidad, se definió en el RFC 3550 el Protocolo de Transporte en Tiempo Real o RTP por sus siglas en inglés (*Real Time Protocol*), el cual es uno de los más utilizados hoy en día para transporte de audio y video. En la Figura 1.10 se muestra la forma en que un paquete RTP es encapsulado en una trama Ethernet. [18], [22]

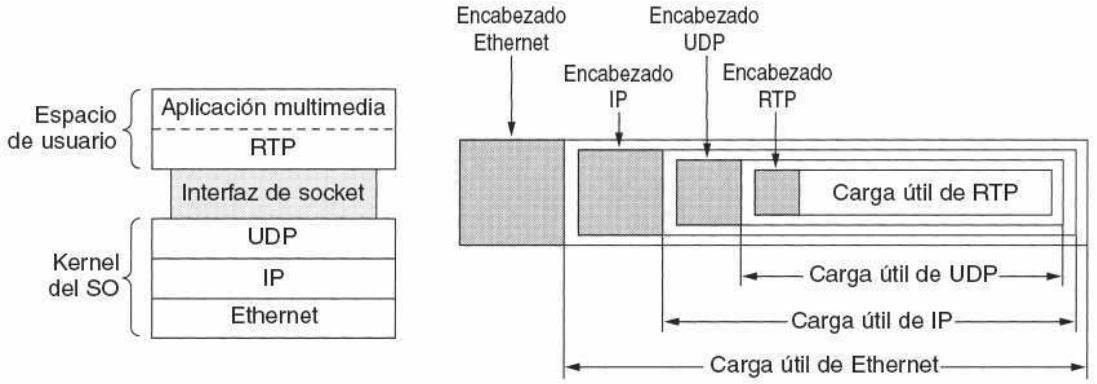


Figura 1.10. Empaquetamiento en RTP [22]

RTP es un protocolo que proporciona funciones de transporte a aplicaciones multimedia. Algunos autores lo describen como un protocolo de transporte, sin embargo, es difícil definir en qué capa se encuentra ya que trabaja de cerca con la capa aplicación en lugar de la capa transporte, donde RTP se encapsula en UDP. [22]

Una de las principales funciones de RTP es transmitir en un solo flujo de paquetes UDP varios mensajes de diferentes aplicaciones multimedia, un trabajo análogo al que realiza UDP sobre IP. Los paquetes RTP son encapsulados en UDP para ser enviados a uno o varios destinos (*unicast* o *multicast*). [22]

Ya que los mensajes RTP son enviados sobre UDP, éstos no tienen un trato especial en la red, a menos que se defina políticas de calidad de servicio. RTP no lleva un seguimiento sobre los mensajes enviados, es decir no implementa mecanismos de control de flujo, control de errores, solicitudes de retransmisión, o confirmaciones de recepción. La carga útil transportada por RTP depende de la aplicación y como ésta desee codificarle. Sin embargo, RTP define perfiles donde asigna un tipo de datos a transportar, y cada perfil puede permitir múltiples formatos de codificación. [22]

Una característica necesaria para la transmisión de aplicaciones en tiempo real es la marcación del tiempo o "*time stamping"* en inglés. Esta característica consiste en identificar con una marca de tiempo cada muestra del paquete, de tal forma que el receptor pueda almacenar los paquetes en un *búfer* antes de entregarlos a la aplicación. La marca de tiempo contiene el momento en que el paquete debe reproducirse luego de iniciada la reproducción. Una vez almacenada una cierta cantidad de paquetes en el *búfer*, éste comienza a entregarlos a la aplicación la cual podrá reproducir cada paquete en el tiempo indicado. Esta característica permite tener un flujo continuo de información multimedia entregado por el *búfer* aún cuando los datos no se reciban en el tiempo esperado. [22]

El Protocolo de Control de Transporte en Tiempo Real, o RTCP por sus siglas en inglés (*Real Time Control Protocol*), trabajan en conjunto con RTP para sincronizar los datos transmitidos y generar retroalimentación acerca de la calidad en la transmisión de RTP. [22]

La sincronización de datos transmitidos y recibidos es especialmente útil cuando el receptor y emisor utilizan relojes de diferente precisión y/o estabilidad, por lo cual pueden presentarse problemas. RTCP es utilizado para mantener estos flujos sincronizados. [22]

La retroalimentación se utiliza para informar al origen acerca de retardos en la transmisión, congestión, ancho de banda disponible, y otras propiedades de la red. Esta característica puede ser utilizada para incrementar la cantidad de información transmitida cuando la red se encuentre disponible, o disminuir en caso de que exista congestión, mejorando así la calidad de transmisión. Otra

ventaja es que esta característica de RTCP permite adaptar el algoritmo de codificación de los datos transmitidos para mejorar la calidad. Por ejemplo, si se encuentra transmitiendo audio MP3 utilizando *PCM*, puede cambiar el tipo de codificación *DELTA*[14]. [22]

Por último, RTCP proporciona una forma para nombrar los diversos orígenes utilizando texto ASCII, por ejemplo. Esta información puede mostrarse en la pantalla del receptor para identificar quien es el origen en ese momento. [22]

1.1.6 CÓDECS DE AUDIO

El proceso para transformar una señal analógica en señal digital y viceversa se conoce como codificación y decodificación. El hardware o software que realiza este proceso se denomina CODEC. Existen definidas diferentes formas de realizar esta conversión, y cada forma difiere en la técnica y ancho de banda necesario luego de la conversión. La mayoría de señalas se codifican utilizando la Modulación por Codificación de Pulsos, o PCM por sus siglas en inglés (*Pulse Code Modulation*), y sus variantes. [70]

Normalmente un CODEC cumple funciones adicionales a la conversión analógica-digital, como por ejemplo la compresión de datos y cancelación de eco. La compresión es una característica importante en enlaces con poco ancho de banda, ya que permite aprovechar el canal con un mayor número de conexiones VoIP simultáneas. Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio, proceso mediante el cual no se transmite nada durante los silencios de las personas en una conversación. La Tabla 1.2 muestra un resumen con los códecs más utilizados en la actualidad. [70], [53]

Nombre	Estandarizado	Tasa de bits (Kbps)	Frecuencia muestreo (KHz)	Periodo de trama (ms)	Descripción
G.711	ITU-T	64	8	Muestreada	PCM
G.721	ITU-T	32	8	Muestreada	ADPCM (Variante de PCM)
G.722	ITU-T	64	16	Muestreada	7 KHz de audio/banda ancha
G.722.1	ITU-T	24/32	16	20	Para sistemas con baja pérdida de paquetes

[14] Es un caso especial de una variante de PCM con una velocidad de muestreo de 32 o 64 kHz.

Nombre	Estandarizado	Tasa de bits (Kbps)	Frecuencia muestreo (KHz)	Periodo de trama (ms)	Descripción
G.723	ITU-T	24/40	8	Muestreada	Extensión del estándar G.721
G.723.1	ITU-T	5.6/6.3	8	30	Doble tasa de codificación para voz
G.726	ITU-T	16/24/32/40	8	Muestreada	ADPCM
G.727	ITU-T	32	8	Muestreada	ADPCM
G.728	ITU-T	16	8	2.5	Utiliza código de predicción de línea
G.729	ITU-T	8	8	10	Combina código de predicción de línea y estructura algébrica
GSM 06.10	ETSI	13	8	22.5	Predicción de excitación pulso regular a largo plazo
LPC10	Gobierno de USA	2.4	8	22.5	Códec predictivo lineal
EVRC	3GPP2	9.6/4.8/1.2	8	20	Códec mejorado de tasa variable
DVI	IMA[15]	32	Variable	Muestreada	ADPCM

Tabla 1.2. Comparación de códecs de voz más utilizados [70]

1.1.7 CENTRAL TELEFÓNICA

En el mundo de la telefonía, convencional o IP, la central telefónica es el corazón del sistema. Una central telefónica es un equipo donde se unen y conmutan todas las conexiones de todos los teléfonos de los abonados de un determinado lugar. La función que realizan las centrales telefónicas es conectar de manera correcta a los abonados al servicio telefónico entre sí. Ponen en contacto al abonado que llama con el destinatario de la llamada (abonado de destino). [58]

Las centralitas telefónicas, o PBX por sus siglas en inglés (*Private Branch Exchange*) pueden ser públicas o privadas. Por lo general el término PBX es utilizado para referir centrales telefónicas privadas administradas y utilizadas dentro de una empresa. Los usuarios del sistema telefónico PBX comparten un número definido de líneas telefónicas con las cuales pueden realizar llamadas hacia la PSTN. Las PBX conectan las extensiones de los usuarios una empresa entre sí y con la PSTN. [28]

[15] Acrónimo de Asociación de Interactividad y Multimedia o *Interactive Multimedia Association* por sus siglas en inglés.

Una de las tendencias más recientes en telefonía es la telefonía computarizada. Esta tecnología convierte a la telefonía en un servicio de red a través del desarrollo de sistemas telefónicos que transmiten la voz utilizando VoIP.

Estos sistemas se los conoce por el nombre de VoIP PBX ó IP PBX. IP PBX no es más que un sistema telefónico basado en software que permite a los usuarios disfrutar de varias funcionalidades y servicios que normalmente son muy costosos y difíciles de implementar con las PBX tradicionales. [28]

1.2 PBX BASADAS EN SOFTWARE LIBRE [30], [34]

En los últimos años el software libre ha comenzado a participar de una forma muy importante en todo tipo de sistemas. Con la aparición de la VoIP, la telefonía ha dado un giro trascendental y sus posibilidades de nuevos servicios se extienden en la medida que las redes evolucionan. Igualmente, las PBX tradicionales se enfrentan hoy a un fuerte competidor, las PBX implementadas con software.

El software libre ha sido el pilar principal para el desarrollo de estas PBX basadas en software, las cuales son capaces de realizar las mismas funciones de una PBX convencional pero a una fracción del costo.

Una PBX basada en software libre es un programa, por lo general con licencia GNU GPL[16], diseñado para cumplir las funciones de una PBX convencional. Este programa se instala sobre un servidor convirtiendo a este equipo en una pequeña central telefónica capaz de gestionar llamadas y, dependiendo del software y la tecnología utilizada, brindar servicios de telefonía.

Diferentes desarrolladores han diseñado este tipo de programas con enfoques particulares, entre los cuales brilla con autoridad ASTERISK por sus características y funcionalidades. [30]

1.2.1 ASTERISK

ASTERISK es una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP mediante todos los protocolos VoIP que implementa. ASTERISK es una aplicación de código abierto basada en

[16] Acrónimo de Licencia Pública General GNU o *GNU General Public License* por sus siglas en inglés.

licencia GPL. Poco a poco, esta aplicación se ha convertido en la evolución de las tradicionales PBX analógicas y digitales permitiendo también la integración con la tecnología VoIP. [30]

Una de las ventajas más atrayentes es su posibilidad de funcionar como sistema híbrido, ya que permite gestionar llamadas telefónicas tradicionales (analógicas, celulares, digitales) como llamadas sobre IP mediante el uso de los protocolos estándar de VoIP. [30]

Uno de los aspectos más interesantes de ASTERISK es que reconoce muchos protocolos VoIP como pueden ser: SIP, H.323, IAX y MGCP. ASTERISK puede funcionar con terminales IP actuando como un servidor *REGISTRAR* y Gateway. Hoy en día en algunos entornos corporativos ASTERISK ha sido adoptado como una gran solución de bajo costo. [30]

La última versión estable de ASTERISK incluye los siguientes módulos: [30]

- *Asterisk*: Ficheros base del proyecto.
- *DAHDI*: Soporte para hardware (antes ZAPTEL).
- *Addons*: Complementos y añadidos del paquete ASTERISK.
- *Libpri*: Soporte para conexiones digitales.

Debido a sus características y funcionalidades, ASTERISK ha sido la base para desarrollar distribuciones de software libre que implementan una interfaz gráfica para la administración de ASTERISK y sus módulos. Entre estas distribuciones se puede destacar: [34], [62], [40], [30]

- FreePBX.
- AsteriskNOW.
- TRIXBOX.
- ELASTIX.

La característica principal de estas distribuciones es la incorporación de una interfaz web para la configuración y gestión de ASTERISK y otros servicios. ELASTIX es una distribución Ecuatoriana estable, desarrollada por la empresa PALO SANTO SOLUTIONS, que ha ganado popularidad en los últimos años; sin

embargo, en el presente trabajo se utilizará ASTERISK sin interfaz gráfica ya que es necesario configurar la PBX de forma personalizada.

1.2.2 ELASTIX

El proyecto ELASTIX se inició como una interfaz de reportes para llamadas de ASTERISK y fue lanzado en marzo del 2006. Posteriormente el proyecto evolucionó hasta convertirse en una distribución basada en ASTERISK que implementa servicios adicionales de telefonía. Por ser una distribución basada en ASTERISK, utiliza su plataforma de comunicaciones. [34]

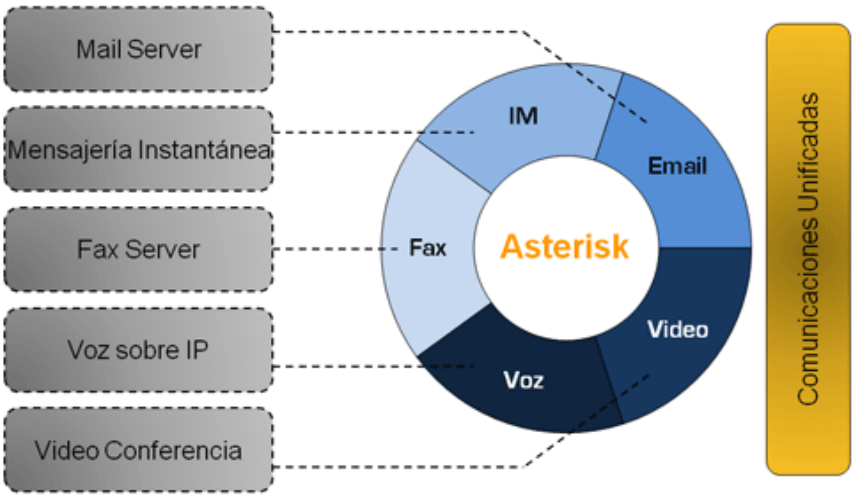


Figura 1.11. Estructura del proyecto ELASTIX [34]

ELASTIX tiene como objetivo desarrollar una distribución de comunicaciones unificadas. Este concepto es más amplio que el de una central telefónica. En este caso, ELASTIX no solamente provee telefonía, integra otros medios de comunicación, servicios y aplicaciones. En la Figura 1.11 se puede observar un diagrama de los servicios que conforman el sistema ELASTIX. [11], [34]

Algunas de las características de ELASTIX son: [34]

- Correo de Voz.
- E-mail y fax.
- Soporte para *softphones*.
- Interfaz de configuración Web.
- Sala de conferencias virtuales.

- Grabación de llamadas.
- Enrutamiento optimizado.
- *Roaming* de extensiones.
- Interconexión entre PBX.
- Identificación del llamante.
- Monitoreo de llamadas.

1.3 DIMENSIONAMIENTO TELEFÓNICO Y ENLACES [24], [25], [51]

Para el diseño e implementación de una PBX es muy importante conocer la capacidad que debe tener para que funcione adecuadamente y un usuario no tenga que esperar para poder realizar una llamada. Existen varias formas estadísticas de analizar el tráfico sobre la red y estimar las capacidades más apropiadas para un enlace. [25]

En este trabajo se hace un pequeño resumen para entender los conceptos básicos del dimensionamiento. Para entender la forma de medir y estudiar el tráfico es necesario conocer las unidades de intensidad. [25], [24]

1.3.1 INTENSIDAD DE TRÁFICO

La unidad básica para medir la intensidad de tráfico es el Erlang. Según la recomendación E.600 de la UIT, en la telefonía tradicional, el número de Erlangs es el número de recursos ocupados o el número de recursos ocupados esperado en condiciones determinadas.

Otra forma de medir la intensidad de tráfico es el Ciento de Segundos del circuito o CCS por sus siglas en inglés (*Circuit Centum Seconds*), que representa la utilización de un circuito durante 100 segundos. La relación entre Erlangs hora y CCS sería: [25], [51]

$$1\ Erlang = 36\ CCS$$

Partiendo de la definición, el tráfico en Erlangs se lo puede calcular encontrando el tráfico total en horas, es decir, sumar el tiempo de todas las llamadas durante un lapso de tiempo y dividiéndolo para el lapso de tiempo en horas. Por otro lado, encontrar el tráfico total en horas puede ser una tarea complicada cuando se tiene

varias líneas que funcionan todo el día, para esto basta con aplicar una fórmula para calcular los Erlangs. [25], [24], [51]

$$Erlang = \frac{\#\ llamadas\ x\ ACHT}{3600}$$

Donde la Constante Tiempo de Duración Promedio de una Llamada o ACHT por sus siglas en inglés (*Average Call Holding Time*) representa el promedio de duración de una llamada en segundos, que normalmente está entre 120 y 180. [24], [51]

GoS	Percepción del servicio por parte del usuario
De 0 a 0.02	De excelente a muy bueno, casi no se rechazan llamadas. El valor 0 no es posible.
De 0.03 a 0.06	De normal a aceptable. Un valor de 0.03 a 0.04 es el más comúnmente usado.
De 0.07 a 0.10	Malo
De 0.10 en adelante	Pésimo, Terrible. Quiere decir que el 10% de llamadas obtendrán ocupado.

Tabla 1.3. Percepción de los usuarios según el grado de servicio o GoS

El Grado de Servicio, o GoS por sus siglas en inglés (*Grade of Service*), es otra variable muy importante y se lo define como la probabilidad de que una llamada falle dado que todos los canales se encuentran ocupados. Un sistema de comunicaciones con todos sus canales ocupados rechazará cualquier llamada adicional a las anteriores, llamadas que se perderán debido a la congestión. En la Tabla 1.3 se presentan los rangos de tolerancia del GoS. [25], [51]

1.3.2 MODELOS ERLANG

En esencia existen dos modelos en las teorías de Erlang que se utilizan con mucha frecuencia en telefonía y son el modelo B y el modelo C. El modelo B se caracteriza por asumir que aquellas llamadas que no consiguen tono de marcado no ingresan a una cola, éste es el caso más real en una PBX. Por su parte, el modelo C se utiliza para calcular probabilidades en llamadas que entran a colas, como es el caso de un CALL CENTER. [25], [51]

1.3.2.1 Erlang B

El modelo Erlang B es el más común para realizar el dimensionamiento de una PBX. En este modelo se asume que una llamada bloqueada no entra a una cola. Es decir que si todas las líneas se encuentran ocupadas el llamante obtendrá tono de ocupado en lugar de ingresar a una cola. [51]

En la Figura 1.12 se muestra el modelo de Erlang B, con un número infinito de llamadas aleatorias y un GoS determinado que brindará servicio a unas llamadas y a otras las bloqueará.

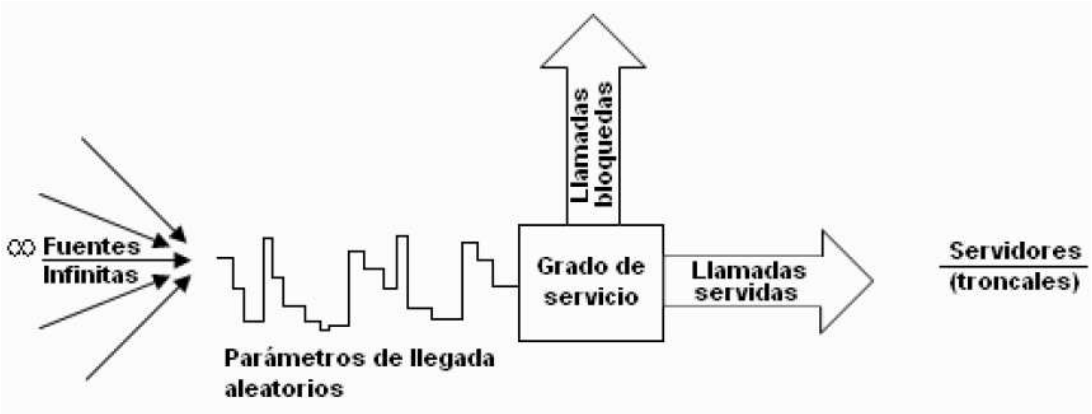


Figura 1.12. Modelo de tráfico para Erlang B [24]

La fórmula propuesta por el modelo Erlang B para el cálculo del GoS es: [11], [25], [24], [51]

$$GoS = \frac{\frac{E^N}{N!}}{\sum_{i=0}^{N} \frac{E^i}{i!}}$$

Donde:

- *E*: Cantidad de tráfico ofrecido en Erlangs.
- *N*: Número de canales en servicio o líneas telefónicas.
- *GoS*: Probabilidad de bloqueo. Este valor está entre 0 y 1.

En esta fórmula se asume que los intentos de llamadas telefónicas llegan aleatoriamente a la central telefónica. Además, las llamadas que no son atendidas son descartadas.

1.4 FRAUDE EN TELEFONÍA [10], [23], [38]

La telefonía, y en general las telecomunicaciones y las redes no se ven exentas de delitos y prácticas ilegales. A la medida que se han desarrollado nuevos equipos y técnicas de comunicación, los delitos han aumentado. La aparición de estas nuevas tecnologías hace que sea más sencillo conseguir los equipos necesarios para cometer un delito en telecomunicaciones.

El mercado de las telecomunicaciones se ha convertido en uno de los más rentables ya que el mundo se ha vuelto extremadamente dependiente de la tecnología. Hace no muchos años, el acceder a Internet o tener un celular era un lujo que pocas personas podían ostentar, si es que existía ya el Internet. La vida de las telecomunicaciones es joven y sin embargo han globalizado el mundo haciéndolo un lugar mucho más pequeño para los negocios y la comunicación.

Esta tendencia mundial aumenta el valor de las telecomunicaciones, y aunque el costo de los servicios disminuye, la medida en que se utilizan los hacen muy atractivos para delitos como el fraude o la estafa. Al hablar de delitos, sean en telecomunicaciones o en informática, se habla de "fraude". Según el diccionario se define el fraude como la "Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete"[17], o el "Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros"[9].

Es importante diferenciar lo que es un delito y una infracción. El delito son aquellas acciones que se encuentran tipificadas en el código penal Ecuatoriano; las infracciones, por otra parte, son aquellas consideradas en la Ley Especial de Telecomunicaciones Reformada y su reglamentación pertinente.

Tanto fraudes informáticos como telefónicos son una práctica ilegal que actualmente no se encuentra considerada con la importancia que merece en las leyes ecuatorianas. Los delitos informáticos en el Ecuador son menos comunes, por ahora, que los delitos en telecomunicaciones, sin embargo el perjuicio que éstos pueden causar es importante, por lo que es necesario establecer leyes que limiten estas prácticas.

[17] Diccionario de la Real Academia de la Lengua, término "Fraude".

En el Ecuador, la SUPERTEL como organismo de control es la entidad estatal que combate activamente este tipo de delitos. Su trabajo lo realiza con base en las leyes y el apoyo de los sectores involucrados, como operadoras telefónicas y usuarios. El móvil más común para cometer un delito en telecomunicaciones es el rédito económico, directo o indirecto. El rédito económico indirecto se refiere a aquellos métodos que no buscan lucro sino evitar el pago del servicio. [10]

El fraude más relevante para el presente trabajo es el conocido sistema telefónico “bypass”. Relacionados al sistema telefónico “bypass”, existen una serie de fraudes, entre los cuales se tiene: [10]

1- Fraude por suscripción.
2- Fraude interno.
3- Fraude de roaming.
4- Refilling.
5- Robo de líneas.
6- Utilización no autorizada de una SIM BOX.
7- Fraude a PBX y *Voicemail*.

1.4.1 FRAUDE POR SUBSCRIPCIÓN

Aunque este fraude involucra el uso de servicios de telecomunicaciones no se trata de un fraude técnico. Se presenta cuando, en el proceso de registro, el usuario presenta documentación falsa o de terceros con el fin de que los cargos por facturación se registren a nombre de otra persona. [10]

Este delito afecta a las personas suplantadas más que a las empresas de telefonía, ya que son reportadas como usuarios morosos a las centrales de riesgo y bases de datos en el sector financiero. Sin embargo, la empresa de telefonía también se ve afectada al no poder cobrar los consumos realizados, tener un aumento en los reclamos, etc. [10]

1.4.2 FRAUDE INTERNO

El referirnos a fraude interno como un tipo de fraude con gran alcance debido a sus diferentes modalidades. En ciertos casos, los autores diferencian los fraudes

internos y externos o al usuario. Para propósitos de este trabajo no es necesaria tal diferenciación.

Estos fraudes son realizados, como su nombre lo indica, desde el interior de las empresas de telecomunicaciones y por lo general involucran personal de las mismas. Los defraudadores pueden utilizar diferentes métodos como alteraciones en los detalles de facturación de un individuo, creación de cuentas falsas, acceso a los detalles de una tarjeta de crédito, daños en elementos de la red, virus o troyanos, etc. Entre los modos más comunes están la asignación no autorizada de líneas de abonado, manipulación de información, y la reventa de facilidades de la central telefónica. [10]

En la asignación no autorizada de líneas de abonado se utilizan líneas de una central telefónica que se encuentren libres, es decir sin asignar a un abonado registrado. Una de estas líneas es utilizada para realizar llamadas o para ser vendida sin la autorización debida por lo que no se registra al usuario. Cuando esta línea es utilizada, los cargos por facturación no son asignados a ninguna persona ya que es una línea sin asignar, y el consume se genera como inconsistencia en el sistema de facturación. [10]

La manipulación de información involucra la parte administrativa de la central telefónica ya que consiste en alterar la plataforma de facturación para borrar o modificar consumos, modificar la base de datos de los clientes para que no se puedan realizar los cobros, o vender información de la compañía. [10]

La reventa de facilidades de la central telefónica consiste en utilizar una línea de propiedad de la central telefónica para realizar llamadas internacionales no autorizadas. Como estás líneas tienen la facilidad de realizar conferencias, se utiliza este sistema para conectar dos destinos internacionales, y facturando las llamadas a la central telefónica. [10]

1.4.3 FRAUDE DE ROAMING

Fraude en *roaming* se lo conoce al uso de un servicio de *roaming* sin la intención de pagar por este servicio. El defraudador contrata una línea en una celular en una operadora nacional utilizando comúnmente fraude por suscripción, luego de

esto activa el servicio de *roaming* y desde el exterior se realizan llamadas a números locales, internacionales o servicios de audio-texto sin la intención de pagar por el consumo. Véase la Figura 1.13.

La facilidad de este fraude se debe al retardo que existe en la transferencia de los registros de llamadas entre las operadoras involucradas en el servicio *roaming*, que puede ser de 72 horas o más para que la operadora de origen reciba la información. Este retardo en el monitoreo crea una ventana que el defraudador, en ataques organizados, puede aprovechar para realizar consumos en cantidades muy significativas.

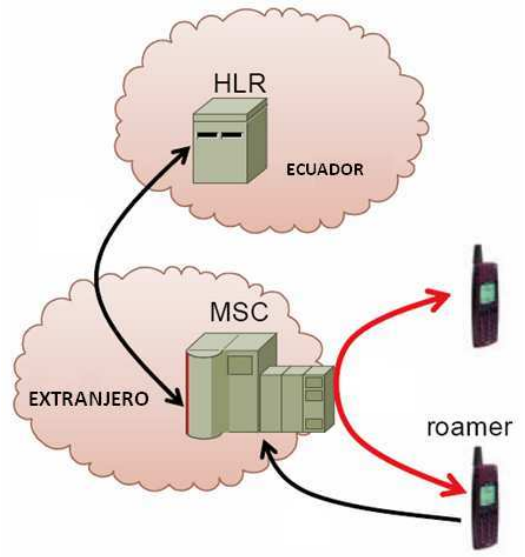


Figura 1.13. Diagrama de fraude de roaming [10]

En este tipo de fraude los operadores se ven bastante afectados ya que no solamente obtienen pérdidas por los ingresos no recaudados de las cuentas utilizadas para el servicio de *roaming*, sino que también asumen las pérdidas por el dinero que están obligados a pagar a sus socios de *roaming*. Estimaciones de algunos sectores del mercado mundial indican que actualmente el fraude de *roaming* representa alrededor del 50% del fraude en GSM.

Este tipo de fraude es bastante atractivo para los defraudadores ya que el servicio de *roaming* es relativamente simple de obtener, ofrece un potencial de altas ganancias debido a los costos de las llamadas que puedan realizar a través de este servicio, y los retardos en la transferencia de la información entre las operadoras involucradas en el servicio de *roaming* facilita escapar a la detección.

1.4.4 REFILLING

Refilling se utiliza para referirse al procedimiento mediante el cual se utiliza un país intermediario con el cual el costo de la conexión al destino se reduce. En este tipo de fraude el país que origina la llamada la encamina a un país intermedio y no directamente a su destino, este punto intermedio direcciona nuevamente la llamada hacia su destino final. [10]

Debido a las diferencias en el costo de terminación de los países involucrados, esta ruta utilizada es más económica que realizar la conexión directa entre el país de origen y destino. El país intermediario genera más tráfico lo que involucra mayores ganancias, sin embargo el país de destino se ve afectado ya que significa una reducción de sus ingresos. [10]

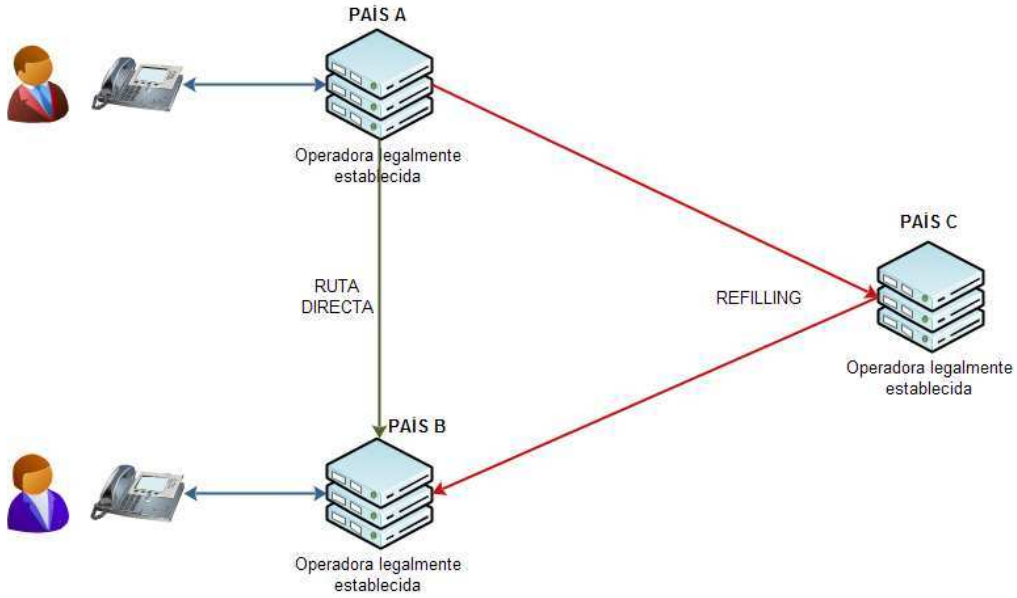


Figura 1.14. Diagrama de un enlace utilizando refilling[18]

Como se puede ver en la Figura 1.14, el *refilling* interno se da entre dos empresas legalmente constituidas lleguen a un acuerdo para que una de ellas direccione tráfico hacia una tercera empresa, aprovechando la diferencia en los costos de interconexión. La operadora A acuerda con la operadora C que todo el tráfico que se envíe hacia la operadora B irá primero hacia C, y esta lo direccionará hacia B. Finalmente, el costo de interconexión entre A y B a través de C resulta más conveniente para la operadora A. [10]

[18] Las figuras o tablas sin referencias han sido generadas por el autor de este trabajo.

Se puede realizar un *refilling* sin el consentimiento de una operadora intermediaria que direccione la llamada. El operador de origen podría hacer uso de un sistema telefónico instalado clandestinamente en el país de la operadora intermediaria. Este sistema por lo general está implementado con VoIP.

Este tipo de sistemas tienen una estructura similar a los denominados sistemas telefónicos “Bypass”, con la diferencia de que no terminan la llamada en el país donde se encuentran funcionando, sino utilizan una operadora legalmente constituida para terminar la llamada en el extranjero. En lugar de utilizar el sistema para terminar ilegalmente una llamada en la red de la operadora local en el país intermediario, realizan llamadas internacionales y utilizan a la operadora local como intermediaria aprovechando el costo de interconexión. Cuando el *refilling* utiliza VoIP, generalmente los defraudadores no tienen relación con las operadoras. [10]

Con base en el diagrama de la Figura 1.14, en este tipo de fraude se ven afectados tanto los intereses de la operadora destino (B) como los intereses de la operadora en el país intermediario (C). La primera por no percibir los réditos de una llamada internacional de mayor costo, y la segunda ya que no sólo encamina llamadas internacionales generadas por ellos, sino también las generadas por el país de origen (A).

1.4.5 ROBO DE LÍNEAS

El robo de líneas es un tipo de fraude donde líneas activas asignadas a abonados de una operadora son cambiadas de domicilio sin autorización del suscriptor o de la empresa proveedora del servicio. Este fraude es muy común por la facilidad de cometerlo en cualquier punto de la red externa, sin embargo suele ser realizado por personas que conocen la red, es decir personal de mantenimiento de la compañía, instaladores o ex trabajadores. [10]

En este tipo de fraude es perjudicado el usuario ya que el consumo realizado por los defraudadores es facturado hacia el usuario registrado a la línea robada. En los casos donde la acometida de la red externa al domicilio del abonado es aérea, es más susceptible a este tipo de fraude ya que puede ser desconectada y llevada a otro lugar. También puede realizarse en un armario desconectando el

par del abonado afectado y empatándolo hacia otro lugar, o en una caja desconectándolo directamente de la troncal. [10]

Si bien el usuario es el principal afectado, la operadora prestadora del servicio se ve afectada por daños que puedan ser ocasionados a su infraestructura y por un aumento de reclamos por parte de los clientes, que además representan un deterioro de la imagen de la compañía frente a sus usuarios.

Por su parte, en muchas ocasiones el usuario no logra comprobar el fraude y/o uso indebido de la línea telefónica por parte de un tercero, por lo que se ve obligado a pagar la factura por el consumo no realizado. [10]

1.4.6 FRAUDE A PBX Y VOICEMAIL

El fraude a PBX ocurre en compañías que cuentan con una PBX conectada a la PSTN. En este tipo de fraude, el defraudador aprovecha un puerto abierto o una falla de seguridad para acceder al sistema de la PBX y originar llamadas sin la intención de pagar. Todo el consumo que los defraudadores realicen es facturado a la empresa. [38]

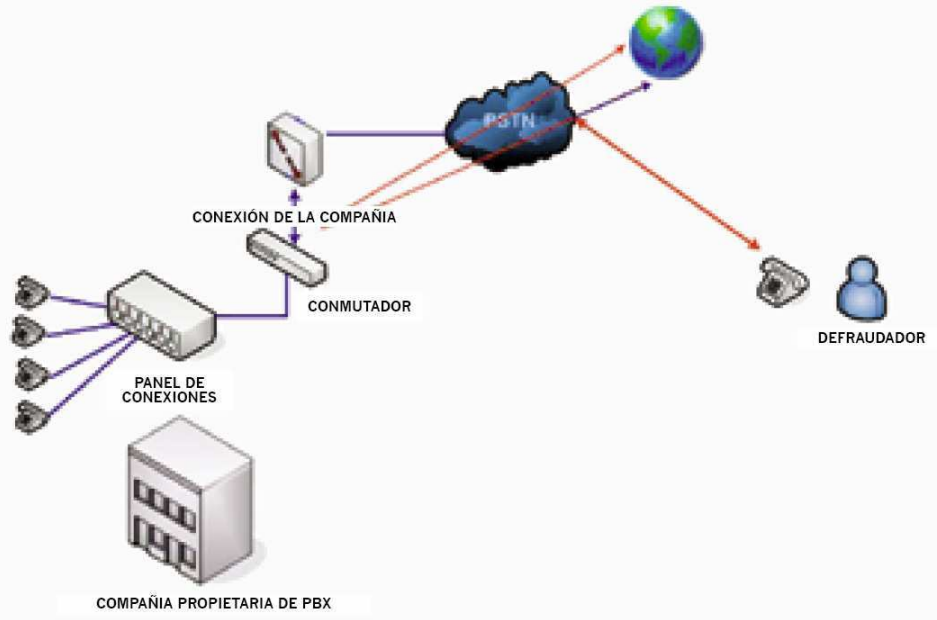


Figura 1.15. Diagrama de un fraude a PBX [10]

Las PBX son configuradas para que los empleados de las empresas, internos o externos, tengan salida a la PSTN a través de las líneas asignadas a la PBX; sin

embargo, los defraudadores se aprovechan registrándose remotamente en la PBX, o a través de sus puertos de Acceso Directo al Sistema, o DISA por sus siglas en inglés (*Direct Inward System Access*), para luego realizar llamadas (locales, internacionales o celulares) que pueden llegar a causar un perjuicio económico alto a la empresa. [10]

En la mayoría de casos quienes realizan el fraude son empleados de la empresa que conocen el funcionamiento del sistema, claves de acceso, etc. Otra forma en que un defraudador puede aprovechar la PBX para realizar llamadas es conectándose de forma remota al equipo. Una vez conectado, puede realizar llamadas y cambiar la configuración de la PBX, alterando los registros del sistema e incluso provocando un mal funcionamiento. [10]

En la Figura 1.15 se puede observar un diagrama de la forma en que un defraudador realiza llamadas a través de una PBX. Los empleados de las empresas son quienes tienen mayor facilidad para realizar este tipo de fraude, sin embargo se debe tener en cuenta que un defraudador puede utilizar "ingeniería social"[19] para obtener información de acceso de los empleados como claves de marcado o registro, para luego ingresar remotamente y realizar llamadas.

Por otra parte, el fraude al correo de voz, o *VOICEMAIL*, es bastante similar. En el 2008, la FCC[20] descubrió un nuevo fraude que permite a los defraudadores usar el sistema de correo de voz de un negocio o usuario, y su clave de acceso predeterminada para hacer llamadas por cobrar sin el conocimiento del usuario, lo cual puede causar un perjuicio sumamente elevado. [38]

1.5 SYSTEMAS TELEFÓNICOS "BYPASS"

De los fraudes telefónicos que se han presentado en el Ecuador, el conocido como sistema telefónico "bypass"[21] es el que más incidencia y consecuencias ha tenido en nuestro mercado de las telecomunicaciones. Este tipo de fraude

[19] "Ingeniería social" es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían.
[20] Comisión Federal de Comunicaciones o *Federal Communications Commission*, por sus siglas en inglés.
[21] Del inglés "bypass", se refiere a una derivación, desvió o ruta alternativa a otra normal.

representa un atractivo para el defraudador dada su rentabilidad en nuestro mercado y ya que en Ecuador aún no se han definido claramente, en sus leyes, las modalidades ilegales de “bypass” y regulaciones que se deben imponer a esta práctica. [10], [19], [20]

El impacto que este tipo de fraude ha tenido tiene relación con dos aspectos de nuestra sociedad, el mercado de telecomunicaciones y las leyes de nuestro país. En algunos países este tipo de sistema telefónico no representa un peligro para las operadoras, dadas sus condiciones de mercado. Sin embargo en el Ecuador es necesario combatir este tipo de ilícitos mientras se actualizan las leyes.

En pocas palabras, un sistema telefónico “bypass” se entiende por un sistema que ingresa una llamada internacional a la red pública conmutada (PSTN), con características de una llamada local. La operadora local interpreta que la llamada es local por lo que la facturación se realiza como llamada local y deja de percibir los ingresos que debería por terminar tráfico internacional.

Figura 1.16. Diagrama de elementos en un sistema telefónico “bypass”

Por su parte, el defraudador se presenta como un proveedor del servicio con ofertas a menor costo, lo que le hace atractivo en la bolsa de tráfico internacional. El operador interesado en terminar tráfico internacional en Ecuador lo ve como una alternativa para ahorrar en el costo de interconexión, e incluso puede llegar a fomentar la instalación de sistemas “bypass” para abaratar costos.

Para la implementación de un “bypass” es necesario tener acceso a la PSTN a través de una línea telefónica que puede ser convencional o celular. En la mayoría de casos, el defraudador consigue estas líneas a través de fraude por suscripción, robo de línea o líneas prepago (operadoras celulares).

El defraudador implementa una pequeña central telefónica que se encarga de recibir el tráfico desde el extranjero y direccionarlo hacia el número destino en el Ecuador a través de una de las líneas telefónicas locales. En la Figura 1.16 se observa un diagrama de la conformación de un sistema “bypass”. La operadora local factura el tráfico local al defraudador mientras este cobra por el tráfico como llamada internacional de menor costo.

1.5.1 CARACTERÍSTICAS DE UN “BYPASS”

Un sistema “bypass” puede ser utilizado para importar o exportar tráfico telefónico. El uso más común en estos sistemas es para importar tráfico (denominado “bypass entrante” por algunos autores), donde se presenta el caso de una central telefónica que ingresa tráfico internacional a la PSTN sin pasar por una operadora autorizada. En la Figura 1.17 se muestra un diagrama de este caso. [10]

Figura 1.17. Diagrama de un “bypass” que procesa llamadas entrantes

Cuando el sistema “bypass” es utilizado para exportar tráfico (conocido como “bypass saliente” por algunos autores), para procesar el tráfico telefónico hacia el extranjero se utilizan tarjetas prepago ilegales, centros de reventa de minutos, comercialización empresarial ilegal, entre otros. En la Figura 1.18 se observa un diagrama de este caso. [10]

Figura 1.18. Diagrama de un “bypass” que procesa llamadas salientes

Entre las principales características de un “bypass” se puede mencionar: [10], [19], [20]

- Grupos de líneas telefónicas en lugar de troncales.
- Enlace internacional que por lo general es el Internet.
- Las líneas utilizadas reciben llamadas en raras ocasiones.
- Las líneas utilizadas generan grandes volúmenes de tráfico, incluso por las noches y fines de semana.
- Ofrece menores costos de terminación de llamada en la bolsa de tráfico internacional, ya que el costo para ellos es de una llamada local.
- Los costos de inversión, operación y mantenimiento son muy bajos en relación con el margen de utilidad.
- La utilización del enlace internacional es simétrica, tanto de subida como bajada de información. Para comunicaciones de voz se requiere un enlace simétrico para garantizar calidad de servicio.

Cada “bypass” tiene características adicionales que dependen del tipo de implementación que tenga, y el modo en que acceda a la PSTN.

1.5.2 FUNCIONAMIENTO DE UN “BYPASS”

En términos generales, un “bypass” está conformado por una pequeña central telefónica, un Gateway de salida internacional, generalmente Internet, y un Gateway de salida hacia la PSTN donde se conectan las líneas telefónicas. [10]

La forma de implementación puede varía según la tecnología que el defraudador utilice, desde enlaces con par de cobre, fibra óptica, o incluso enlaces inalámbricos no autorizados. [10], [19], [20], [23]

En la Figura 1.19 se puede observar un diagrama de una ruta internacional autorizada. En primer lugar, el proceso que sigue una llamada internacional al realizarse a través de una ruta autorizada tiene varias etapas: [23]

1- Un usuario que desea realizar una llamada internacional utiliza tarjetas de telefonía o una operadora autorizada para marcar el código de llamadas internacionales y el número destino en el extranjero.
2- La llamada ingresa en la operadora local, la cual la direcciona hacia un *carrier* internacional con quien mantiene un acuerdo para direccionar llamadas internacionales.
3- El *carrier* internacional direcciona la llamada hacia la operadora de telefonía en el país de destino a través de su red. En algunos casos la llamada pasa por una estación terrena y una central de facturación antes de terminar en el operadora del país destino.
4- El operador en el país destino direcciona la llamada a su usuario final a través de la PSTN local.

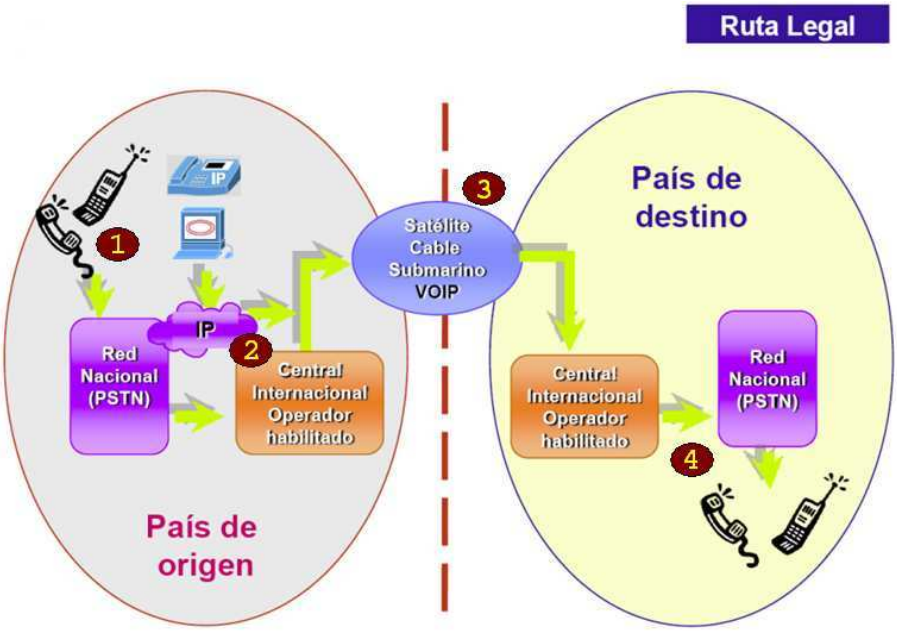


Figura 1.19. Llamada internacional a través de una ruta autorizada [23]

De igual forma, el proceso de una llamada internacional que se realiza a través de una ruta no autorizada o “bypass” tiene varias etapas. En la Figura 1.20 se puede observar un diagrama de una ruta internacional no autorizada o “bypass”. La llamada internacional puede tener dos caminos, dependiendo de si se trata de un

bypass que importe o exporte tráfico. Los “bypass” que importan tráfico, o “bypass” entrantes, siguen el siguiente proceso: [10]

1- Un usuario que desea realizar una llamada internacional, utilizando tarjetas de telefonía internacionales o a través de una operadora, marca el código para llamadas internacionales y el número destino en el extranjero.

2- La llamada ingresa en la operadora local, la cual la direcciona hacia un *carrier* internacional con quien mantiene un acuerdo para direccionar llamadas internacionales.

3- El *carrier* internacional, quien ha llegado a un acuerdo con un defraudador en la bolsa de tráfico internacional, direcciona la llamada hacia la central telefónica del defraudador en el país de destino.

4- El defraudador recibe el tráfico y lo direcciona hacia el usuario final en la PSTN del país destino utilizando una de las líneas locales adquiridas para cometer el ilícito. Para la operadora destino la llamada se origina y termina en la misma operadora, por lo que es una llamada local.

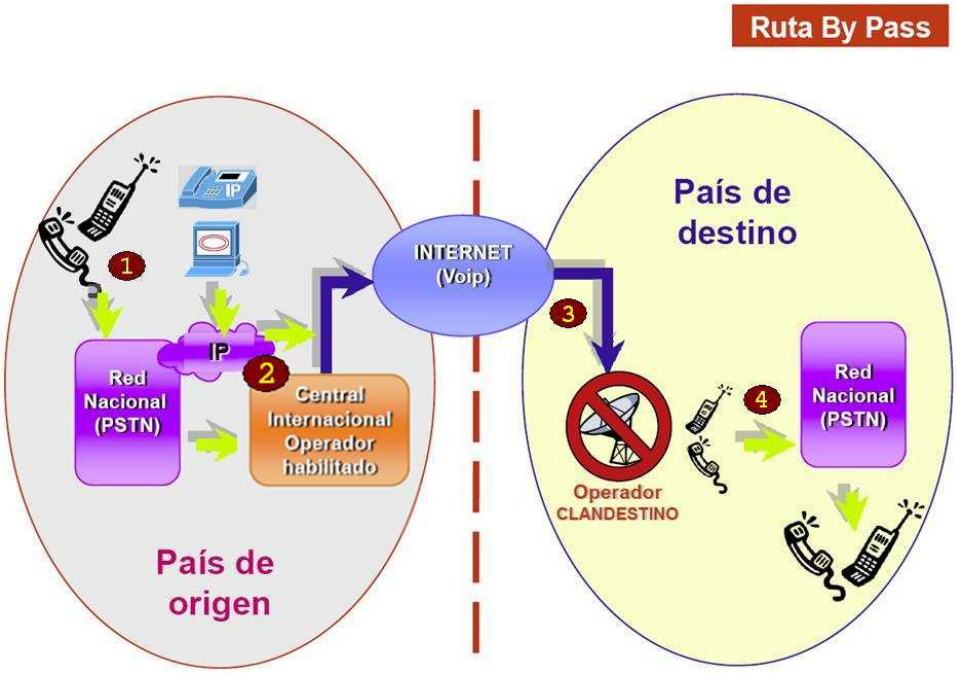


Figura 1.20. Llamada internacional a través de una ruta no autorizada [23]

Hoy en día, los *carriers* internacionales, en su mayoría, transportan tráfico de VoIP por lo que el defraudador recibe el tráfico como VoIP y realiza la conversión

para realizar la llamada local, en caso de que la PSTN local utilice tecnología analógica.

Por otro lado, los “bypass” que exporta tráfico telefónico o “bypass” salientes, siguen los siguientes pasos, como se observa en la Figura 1.21: [10]

1- Un usuario que desea realizar una llamada internacional, por lo general utilizando tarjetas de telefonía realiza una llamada hacia un número según las instrucciones de la tarjeta. Este número puede ser local o internacional.

2- La llamada ingresa en la operadora local y es direccionada hacia el número marcado. Este número conecta con una operadora ilegal que convierte la llamada en VoIP y la entrega a un *carrier* para que la direccione hacia su país destino.

3- El *carrier* internacional direcciona la llamada a través de su red hacia la operadora de telefonía en el país de destino con quien tiene un acuerdo para terminar tráfico internacional.

4- El operador en el país destino recibe la llamada internacional y la direcciona a su usuario final utilizando la PSTN local.

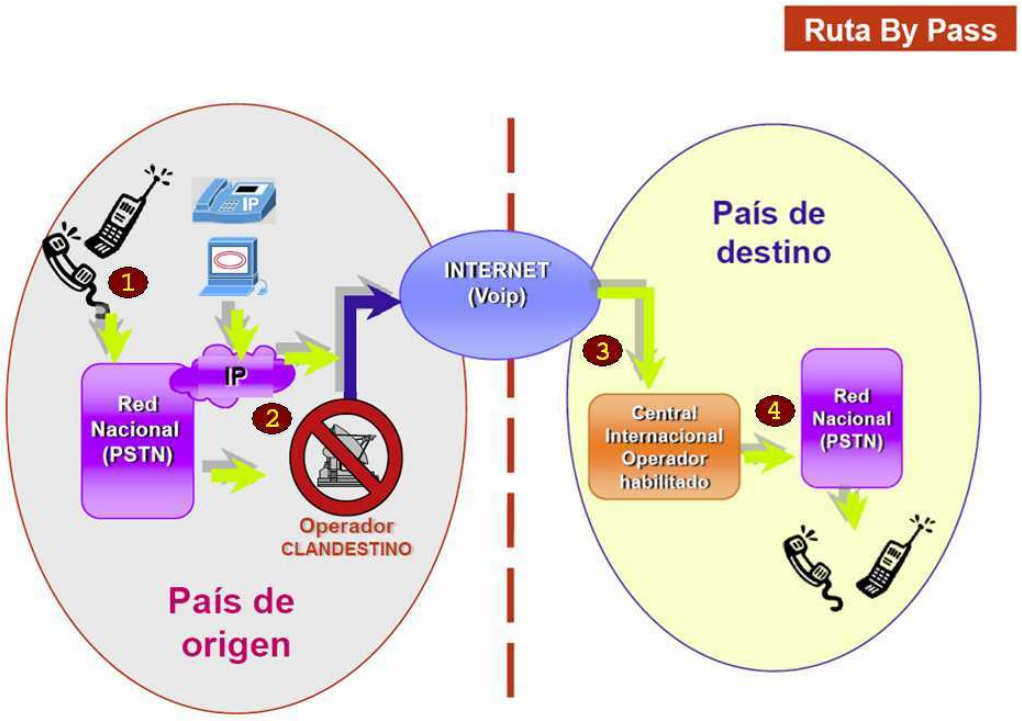


Figura 1.21. Llamada internacional a través de una ruta no autorizada [23]

Algunos de los pasos o rutas que sigue el tráfico pueden variar según la modalidad de “bypass” implementado.

1.5.3 TIPOS DE “BYPASS”

Para fines de este trabajo resulta conveniente clasificar a los “bypass” por su forma de acceder a la PSTN, sin hacer énfasis en la tecnología que se utilice.

1.5.3.1 Líneas convencionales y cuentas

En este tipo de “bypass” el defraudador adquiere varias líneas de una operadora local de telefonía fija o una cuenta con varios números telefónicos (posiblemente utilizando fraude por suscripción). Luego conecta su central no autorizada a estas líneas y la configura para que las llamadas entrantes del enlace internacional se conecten a la PSTN a través de esas líneas.

1.5.3.2 Locutorios y líneas de cabinas públicas

Una modalidad que ha tomado algo de fuerza en los últimos años es el utilizar cabinas públicas y locutorios autorizados para camuflar un sistema “Bypass”.

En esta modalidad los locutorios ofrecen el servicio de llamada nacional e internacional y al mismo tiempo utilizan la infraestructura, en algunos casos propiedad de la operadora, para implementar un sistema “bypass”. [10]

Cuando esta modalidad de fraude se presenta en un locutorio, se compromete al dueño del mismo quien es el responsable por el uso que se les da a los equipos; razón por la cual esta modalidad no se ha popularizado. [10]

Por otra parte, las cabinas también pueden ser objeto de robo de líneas para utilizarlas en sistemas “bypass”. En este caso dichas cabinas pueden verse afectadas si el defraudador daña el terminal a fin de apropiarse de la línea. [10]

1.5.3.3 Líneas celulares

Otra forma de acceder a la PSTN es a través de líneas celulares. En este tipo de fraude las operadoras de telefonía celular son el principal blanco de los defraudadores ya que el tráfico internacional es direccionado hacia sus redes sin la autorización de la operadora. [10]

En esta modalidad se utiliza un equipo conocido como SIM BOX que permite utilizar un grupo de tarjetas SIM[22] simultáneamente para cometer el ilícito. Cuando se desea establecer una llamada, el equipo selecciona automáticamente la SIM por donde se realizará la misma. Dependiendo de la capacidad de la SIM BOX, ésta puede contener hasta cientos de tarjetas SIM. [10], [19], [20]

Las tarjetas SIM utilizadas son planes PREPAGO y pueden conseguirse en cualquier punto de venta del operador ya que para adquirir este tipo de tarjetas no es necesario firmar un contrato o verificar la identidad del comprador, como en los planes POSTPAGO. Estas tarjetas son cargadas con un saldo inicial, y utilizadas según la cantidad de saldo disponible. Una vez terminado el saldo son desechadas y reemplazadas por nuevas tarjetas. [10]

En esta modalidad de "bypass" la detección es relativamente sencilla ya que el comportamiento de lo radio base donde se encuentra ubicado el "bypass" cambia en relación a los volúmenes normales de tráfico. Sin embargo, es un poco más complicado determinar la ubicación geográfica del sistema por su característica de acceso inalámbrico. No obstante, existen técnicas que pueden reducir el área más probable donde se encuentra el equipo, por ejemplo haciendo uso de equipos de triangulación o radiogoniometría (estos sistemas se encuentran en fase de prueba en la SUPERTEL).

Una SIM BOX utilizada en estos sistemas habitualmente maneja alto volumen de tráfico, operan Gateway GSM/IP, soportan interfaces analógicas, ISDN, VoIP, IP, etc., y permiten agregar módulos de tarjetas SIM.

1.5.4 SISTEMAS "BYPASS" CON SOFTWARE LIBRE

Como se ha detallado anteriormente, el principal elemento de un sistema "bypass" es la central telefónica que direcciona el tráfico internacional hacia la red pública. Esta central telefónica puede ser implementada en base a equipos dedicados para esto o en base a software de telefonía sobre un servidor.

[22] El Modulo de Identidad del Abonado o SIM por sus siglas en inglés (*Subscriber Identity Module*) es una tarjeta inteligente desmontable usada en teléfonos móviles y módems USB. Esta tarjeta se utiliza en tecnología GSM.

Como se ha visto, existe una variedad de software en el mercado que permite la implementación de centrales telefónicas privadas a bajo costo y fácil configuración. Esta nueva alternativa abre nuevas posibilidades para la implementación de “bypass” utilizando software libre, abaratando costos y haciéndolo más accesible.

Es importante mencionar que este tipo de sistemas podrían utilizar cualquier tipo de “bypass” de los mencionados. La implementación de este sistema permite al defraudador configurar y tener mayor control sobre el mismo, además que casi todo el equipo necesario para hacerlo está al alcance de cualquier persona.

1.6 DISEÑO DE SOFTWARE [9], [16], [66]

Al diseño de software se lo puede entender como una representación metódica de los procesos necesarios para brindar a una necesidad real, una aplicación que la supla. El estudio del diseño de software es conocido como Ingeniería de Software, cuyo principal objetivo es desarrollar software de calidad. En la Ingeniería de Software, el diseño es el primer paso en la producción de una aplicación. [16]

El diseño de software es la fase preliminar a la implementación; aquí se analizan las necesidades y se elabora una representación de la solución. Tradicionalmente, el diseño de software está ligado a métodos estructurados como la programación orientada a objetos; sin embargo, existen métodos alternativos como la Programación Extrema, o XP por sus siglas en inglés (*Extreme Programming*). En este método de programación el software se desarrolla en etapas, donde cada etapa busca satisfacer una parte de la necesidad del usuario. [66], [16]

Todos los métodos de diseño y programación concuerdan en la importancia de desarrollar soluciones de calidad. Para esto es importante considerar algunos aspectos percibidos por el usuario: [66], [16], [1]

- *Confiabilidad*: Es la capacidad de un software para cumplir con todas las funcionalidades detalladas en las especificaciones, y responder adecuadamente en errores o situaciones inesperadas.

- *Extensibilidad*: Esto es su característica para adaptarse a cambios de especificaciones o necesidades. Está relacionado a la modularidad del software.
- *Reutilización*: La capacidad de utilizar el programa, o alguna de sus partes, en nuevas aplicaciones.
- *Compatibilidad*: La característica de un software de funcionar con otras aplicaciones.
- *Eficiencia*: La utilización que genera un software de los recursos de un computador, almacenamiento de datos y memoria, siendo dejar de ser rápido. A menor utilización, mayor eficiencia.
- *Portabilidad*: La facilidad de una aplicación de funcionar en diferentes plataformas.
- *Funcionalidad*: Las funciones y tareas que puede realizar el programa. Esto está estrechamente relacionado a las necesidades del usuario.
- *Facilidad* de uso: La facilidad con que diferentes usuarios, con distintos niveles de conocimiento entienden el funcionamiento de una aplicación y aprenden a utilizarla.

1.6.1 PROGRAMACIÓN ORIENTADA A OBJETOS

El concepto de objeto es muy utilizado en la programación para crear abstracciones de la realidad. Explicar el término “objeto” en software puede resultar confuso y frustrante, sin embargo un ejemplo aclara la idea. Supongamos una mesa; Una mesa es un objeto específico que puede pertenecer a un grupo general, o clase, llamada muebles. La mesa contiene los atributos y funciones que determinados en la clase muebles. [66], [1]

Como podemos ver en la Figura 1.22, un objeto recibe todos los atributos y operaciones de la clase a la que pertenece, y cada objeto tendrá su propio valor para cada atributo.

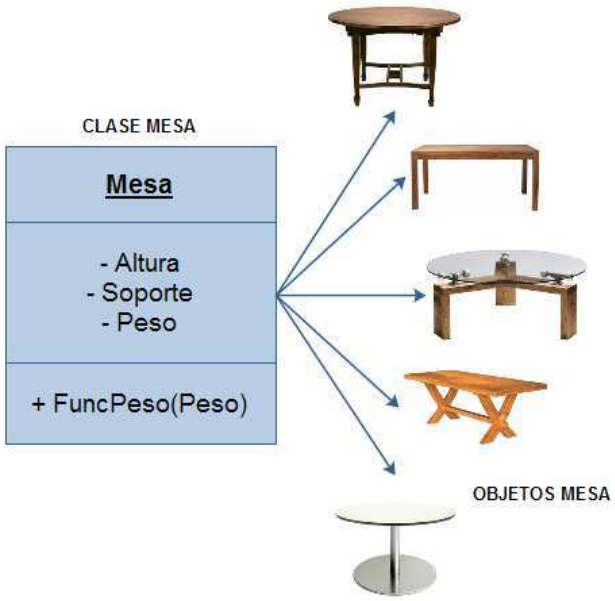


Figura 1.22. Representación de clases y objetos UML

Como en la vida real, cada objeto tiene sus propias características y funciones, aunque muchas de estas sean compartidas en objetos similares. [66]

1.6.1.1 Clase y Objeto

Basándonos en el ejemplo anterior, una mesa por si sola puede tener una serie de características que la distinguen de otras mesas. Así mismo existen una variedad de tamaños y formas para mesas, aunque a todas se las puede definir y diferenciar evaluando una serie de atributos que todas tienen, como el número de patas, el tipo de soporte, tipo de superficie, material, etc. Al grupo general de mesas se lo denomina Clase. [66], [9]

En otras palabras, una Clase es una abstracción general de un grupo de objetos que comparten una serie de atributos. Cada objeto es una instancia de una clase y contiene los atributos y funciones definidos en la clase. Un auto de dos puertas, un sedán, un todo terreno, etc., son instancias de una clase “Automóvil”. [66]

1.6.1.2 Herencia

El concepto de herencia es sumamente importante en la programación orientada a objetos. En ciertas ocasiones, una clase no es suficiente para definir objetos muy particulares o con atributos únicos, sin embargo comparten sus otros atributos con los demás objetos. En este caso se pueden heredar los atributos y

funciones (métodos) de una clase a una subclase, en la cual los objetos instanciados tendrán todos los atributos heredados de la superclase, además de sus atributos propios. [66]

Como ejemplo tomemos un automóvil. La clase *Automóvil* define los atributos generales para todos los automóviles, sin embargo una camioneta puede tener su capacidad de carga como atributo propio diferente a otros objetos de la clase *Automóvil* como un sedán o un auto deportivo.

Es necesario entonces definir una subclase *Camioneta* que tendrá como superclase la clase *Automóvil* y heredará todos sus atributos y funciones. [66], [9]

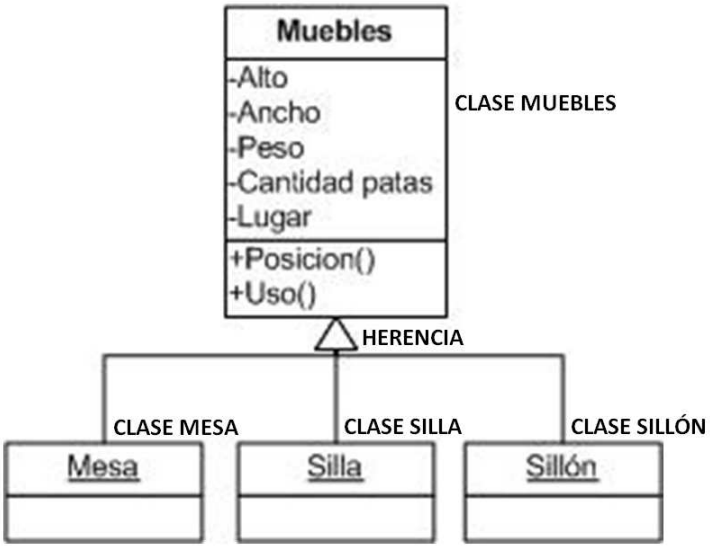


Figura 1.23. Representación de clases y herencias en UML [66]

En la Figura 1.23 se observa una relación de herencia, donde las subclases silla, mesa y sillón heredan todos los atributos y funciones de la superclase *Muebles*, y además definen sus propios atributos que las hacen diferentes entre ellas. [66]

1.6.1.3 Métodos

Los objetos, y por ende las clases, contienen valores y realizan operaciones. A estas operaciones o funciones se las conoce como Métodos, es decir que cada método es una representación de una operación que el objeto realiza. Cada método puede ser sencillo, como devolver el valor de algún atributo del objeto, o complejo como para alterar valores o generar operaciones. [9]

Por ejemplo, un método para una mesa puede ser “conocer peso”, que devuelva el valor del peso de la mesa.

1.6.1.4 Mensajes

Los mensajes son el medio que utilizan los objetos para comunicarse entre sí. Como en el mundo real, los objetos interactúan entre ellos, y muchas veces el resultado de una operación en un objeto es necesario para dar paso a la operación de otro. [9]

En los mensajes que se envían a un objeto se especifica el objeto destino, seguido del método que sea requerido y los valores para que dicho método se lleve a cabo. El objeto destino realiza sus operaciones definidas en el método, y de ser el caso da una respuesta. [9]

1.6.2 PROGRAMACIÓN ORIENTADA A COMPONENTES

La programación orientada a componentes es considerada una evolución de la programación orientada a objetos. Nace de la idea de reutilizar aplicaciones ya existentes para optimizar el trabajo y obtener resultados de buena calidad con menor esfuerzo y en menor tiempo. [68]

En el desarrollo de software, es muy común que las aplicaciones tengan que ser escritas en su mayoría, pese a librerías y *frameworks* existentes. Este trabajo puede ser minimizado en el concepto de componentes, donde cada aplicación debe ser estructurada pensando en que estará formada por componentes que interactúan entre sí, y pueden ser reutilizados par otras aplicaciones. [68]

Sin embargo, para cumplir con estos objetivos se debe mantener estándares de programación que definan la forma en que los componentes interactúen. Implementar componentes tiene una serie de beneficios como el ahorro de tiempo y esfuerzo, además que garantiza aplicaciones sólidas y con un mínimo de errores ya que los componentes que se distribuyen son sometidos a rigurosas pruebas. [68]

Otro beneficio de los componentes es que pueden ser desarrollados en cualquier lenguaje y de igual forma pueden ser utilizados por cualquier lenguaje.

1.6.3 LENGUAJE UML

El Lenguaje Unificado de Modelado, o UML por sus siglas en inglés (*Unified Modeling Language*) es un lenguaje que sirve para implementar el modelo de un software, visualizar sus componentes, especificar sus funciones y documentar la estructura de sistemas de cualquier tamaño. Entiéndase que UML no es una técnica de diseño sino una herramienta estándar que permite escribir los componentes de una aplicación de forma clara y ordenada. [66], [16]

UML es un lenguaje independiente del método de diseño que se utilice, sin embargo es recomendable utilizarlo en procesos dirigidos por casos de uso. UML es un estándar donde se especifica la forma y reglas para modelar un software, por lo que es utilizado tanto para la implementación conceptual como la física del sistema. [16], [9]

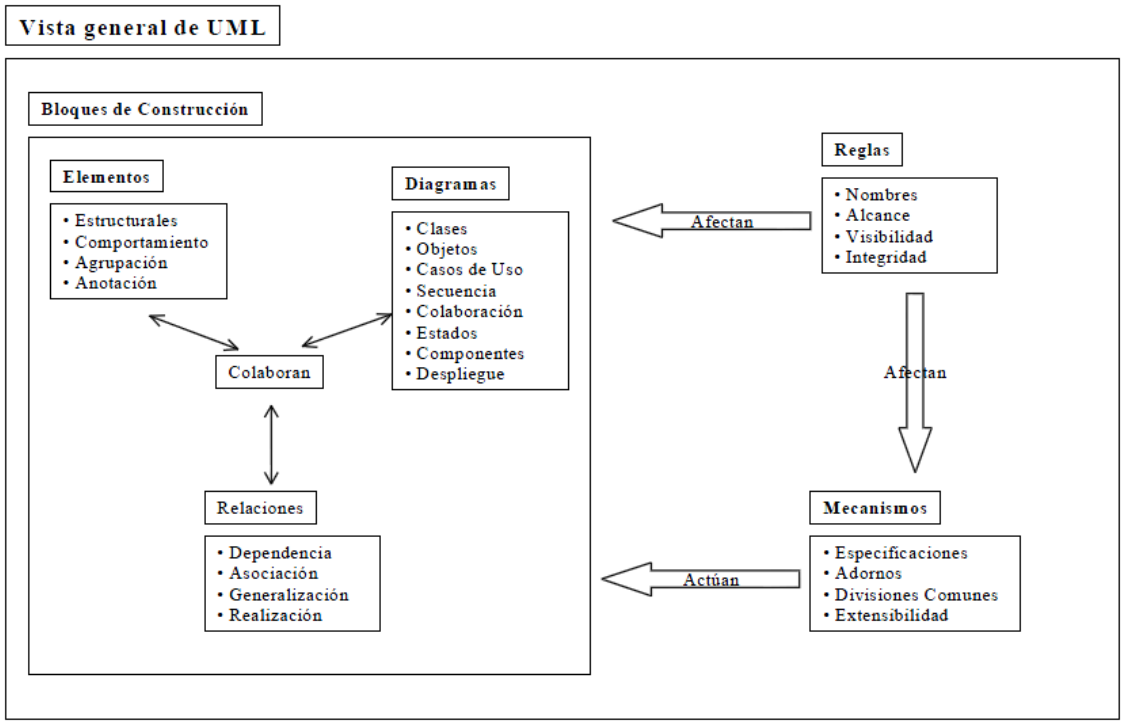


Figura 1.24. Vista general de los elementos del lenguaje UML [9]

Una solución de software descrita utilizando UML contiene cuadros y diagramas conceptuales que facilitan la comprensión de la estructura de una aplicación y permite implementar o afinar el software de forma sencilla. Sin embargo, este lenguaje puede ser utilizado como parte de la ingeniería de software en la etapa

de diseño para luego proceder a la implementación; o de forma inversa, a partir de un software ya implementado. [16]

En el estándar UML se definen tres elementos principales, los bloques de construcción, las reglas, y mecanismos comunes. Los bloques de construcción se dividen en Elementos, Relaciones y Diagramas que permiten describir los objetos de un sistema y sus relaciones. En la Figura 1.24 se puede observar un diagrama de la relación entre estos elementos. Las reglas son convenciones que determinan aspectos como las características de los nombres, alcance de éstos, visibilidad entre ellos, etc. Finalmente, los mecanismos permiten que el lenguaje sea adaptado por cada persona a su necesidad. Para esto se proporcionan especificaciones de los bloques, adornos y divisiones comunes, entre otros. [16]

1.6.4 PROGRAMACIÓN EXTREMA

La Programación Extrema, o XP por sus siglas en inglés (*Extreme Programming*), es una técnica para el desarrollo de software que no utiliza los métodos tradicionales de modelado. En su libro “eXtremeProgramming”, José Carlos Cortizo Pérez basándose en otros autores define a la programación extrema de la siguiente forma:

> *“… se podría decir que la programación extrema es una metodología ligera o ágil para el desarrollo de software eficiente y altamente efectivo*”

Uno de los principales objetivos de XP es la simplicidad en el desarrollo de los sistemas. Los programadores deben tener comunicación constante con el cliente y probar periódicamente el software para continuar adecuándolo, corrigiéndolo y mejorándolo. [37]

Esta idea permite que el cliente tenga mayor poder de decisión sobre la aplicación que obtendrá ya que en cada prueba puede sugerir cambios o adecuaciones al software, los cuales se implementarán en siguientes etapas y podrán ser probados antes de su aprobación final. Esto provee flexibilidad para responder a cambios de diseño o necesidades.

XP, como en toda metodología, define ciertas reglas para su utilización. Algunas de estas reglas pueden ser objeto de análisis según cada grupo de trabajo; no obstante, son una guía para quienes optan por esta metodología: [37]

- *Planificación*: La planificación consiste en escuchar las necesidades del usuario y preparar el diseño para iniciar el trabajo. Los programadores deben ajustarse al diseño y evitar añadir código que no esté contemplado y que probablemente en un futuro deba ser retirado.

- *Diseño*: En la programación extrema el diseño debe ser simple y eficiente. Se debe considerar una buena plataforma para representar el diseño y explicarlo al grupo. En esta parte, se establece que ningún código será agregado con anterioridad.

- *Codificación*: El código que se utilice debe estar dentro de los estándares. También se establece que la programación debe realizarse en parejas y de modo compartido. Es necesario contar con una computadora para publicar las versiones del programa que vayan siendo desarrolladas.

- *Pruebas*: Todo el código debe contar con unidades de prueba calificadas, y debe pasar esas pruebas para lanzar una versión. Si se encuentran errores se debe definir pruebas para identificar el error y corregirlo. Las pruebas que se realicen y los puntajes obtenidos deben ser publicados.

- *Administración*: Como todo proyecto, la administración debe ser considerada de mucha importancia para manejar el equipo de trabajo, hacer un seguimiento a los objetivos y tiempos, y corregir aspectos que sean necesarios en la organización del grupo.

1.7 LENGUAJES DE PROGRAMACIÓN [8], [45], [52]

1.7.1 VISUAL STUDIO

Visual Estudio es un entorno gráfico de desarrollo de software propiedad de Microsoft. Soporta una serie de lenguajes de programación como Visual Basic, C#, ASP .NET, etc. Es utilizado por muchos programadores que trabajan con

programación orientada a objetos, por su amplia plataforma con librerías que facilitan la programación.

Los diferentes entornos y lenguajes que ofrece Visual Estudio son:

- Visual Basic.
- Visual C#.
- Visual C++.
- ASP.NET.

1.7.2 JAVA

Java es un lenguaje de programación orientado a objetos basado en la sintaxis de C y C++. Fue desarrollado por *Sun Microsystems* como una solución simple que utiliza librerías de medio y alto nivel, descartando casi por completo el lenguaje de bajo nivel. [45]

Una de las características que hace de Java un lenguaje singular es su característica de movilidad, es decir multiplataforma. Java funciona sobre un entorno conocido como *Java Virtual Machine* (JVM) o *Máquina Virtual Java* que puede ser instalado y ejecutado en prácticamente cualquier sistema operativo. Este entorno permite de igual forma ejecutar aplicaciones *Java*, es decir, una aplicación java puede ejecutarse sobre cualquier plataforma. [8]

La JVM se encarga de crear una interfaz entre el Sistema operativo donde se ejecuta una aplicación Java y la aplicación. Esta máquina virtual se encuentra escrita de acuerdo al sistema operativo y compila las aplicaciones Java utilizando bibliotecas que le permiten acceder a las funciones del sistema operativo en el que trabaje. [45], [8]

Otra característica de Java es la facilidad que ofrece para desarrollar aplicaciones para dispositivos móviles como *Smart Phones*, gracias a su entorno de desarrollo *Java ME*. De igual forma, se pueden programar aplicaciones WEB, de escritorio con entorno gráfico, *servlets*, aplicaciones para navegadores WEB (*JavaFX*), etc. [45], [8]

El trabajo con hilos, o multitarea, es una característica de este lenguaje. Java tiene un conjunto de bibliotecas que hacen posible un manejo de hilos rápido y sencillo. Además, Java está bajo Licencia Pública General de GNU, o GNU GLP por sus siglas en inglés (*GNU General Public License*), lo cual facilita su uso. [8]

1.7.3 PHP

El Preprocesador de Hypertexto, o PHP por sus siglas en inglés (*Hypertext Preprocessor*), es un lenguaje de programación orientado a objetos desarrollado para crear páginas WEB dinámicas. Una de los principales usos que tiene PHP es la conexión a bases de datos para realizar consultas a través de una página WEB. El código PHP contenido en una página WEB se ejecuta del lado del servidor y el resultado se envía al cliente a través del protocolo HTTP. [52]

PHP es un lenguaje independiente de la plataforma y soportado sobre los principales servidores WEB como Apache, Microsoft IIS y Personal Web Server. Es importante destacar que PHP ofrece varias funcionalidades como programar scripts para páginas WEB, las cuales son: [52]

- Scripts del lado-servidor: Es el principal uso que tiene PHP y consiste en ejecutar código en el lado del servidor a través de una página WEB. Con un motor PHP y un servidor WEB, el código PHP se incluye en las páginas para ser ejecutado cuando la página lo requiera.

- Scripts en la línea de comandos: PHP puede ser utilizado para crear scripts y ejecutarlos sin necesidad de un navegador WEB, tan solo con un intérprete PHP en el servidor.

- Aplicaciones con interfaz gráfica: PHP permite desarrollar aplicaciones cliente con interfaz gráfica utilizando la extensión PHP-GTK. Sin embargo, PHP no fue diseñado originalmente con este propósito.

El lenguaje PHP es muy similar a C o C++; sin embargo, una desventaja es su característica de no proveer scripts multitarea, es decir, no maneja hilos. PHP tiene grandes ventajas pero está orientado principalmente al desarrollo de

páginas WEB dinámicas y conexión a bases de datos en lugar de aplicaciones distribuidas. [52]

1.7.4 CONSIDERACIONES DE LOS LENGUAJES

Definir que lenguaje se utilizará para una solución tiene relación con las necesidades del programador y del problema. Puede ser que más de una herramienta facilite el trabajo y permita cumplir con los objetivos de un programa. Para fines de este trabajo, se consideran dos posibles herramientas: *JAVA* y *PHP*. Como se ha analizado, ambas utilizan el concepto de programación orientada a objetos que se aplicará en esta solución, y a diferencia de *Visual Studio*, son gratuitas.

En síntesis, PHP es una herramienta basada en C que corre sobre código *HTML*, es decir sobre páginas WEB. PHP se ha vuelto muy popular y su característica más notable es que se ejecuta del lado del servidor, enviando los resultados al cliente a través de la WEB. Es muy práctico para mostrar resultados e interactuar con el cliente del servicio dado su entorno gráfico, pero tiene limitaciones en cuanto al manejo de hilos, los cuales son necesarios para este trabajo. Además, PHP es un lenguaje que se ejecuta principalmente cuando una página WEB que es abierta, y no como una aplicación independiente.

JAVA es un lenguaje basado en software libre que, al igual que PHP, es independiente del S.O. en el que se lo ejecute. La programación en JAVA ha ganado popularidad por ser orientada a objetos, multiplataforma, y bajo licencia GNU GPL. Este lenguaje es utilizado para desarrollar aplicaciones de escritorio y distribuidas. JAVA es muy útil para esta solución por el manejo de hilos que implementa. Adicionalmente, al desarrollar una aplicación distribuida se deben considerar posibles problemas de seguridad en la conexión del cliente con el servidor.

CAPÍTULO 2

ANÁLSIS DE LA SITUACIÓN ACTUAL

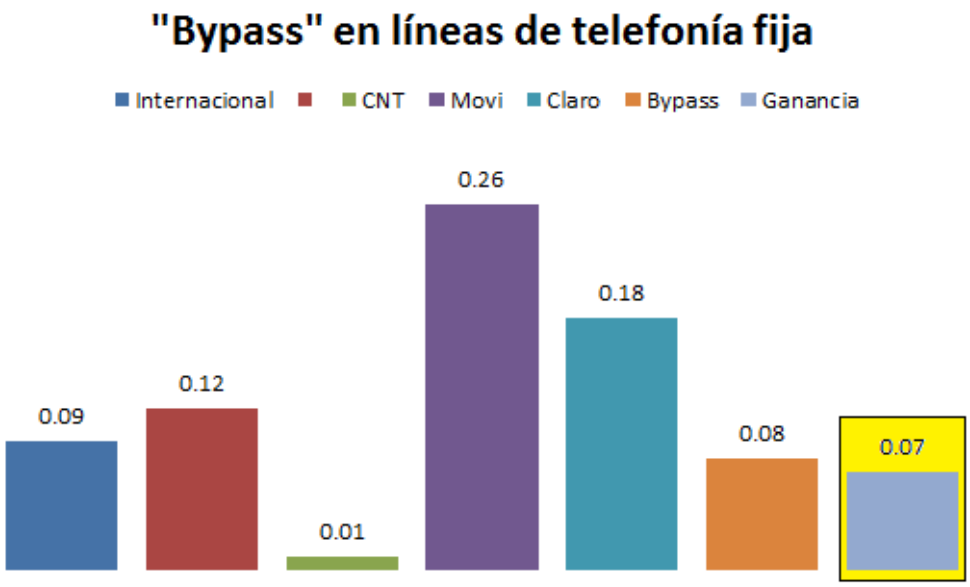
2.1 TÉCNICAS PARA EL CONTROL DE "BYPASS" [7], [10], [21]

La lucha contra los ilícitos en telecomunicaciones, en este caso los sistemas "bypass", no solamente busca detener a defraudadores, sino proteger el mercado y sus actores involucrados que se ven afectados por este tipo de práctica ilegal. El "bypass" afecta tanto a la operadora que brinda el servicio como al Estado y los usuarios del mismo. Más adelante se hará un pequeño análisis del impacto que ha tenido este tipo de fraude en el mercado ecuatoriano.

En la tarea de cuidar el mercado de las telecomunicaciones haciendo frente a estos ilícitos no basta con detectar y desmantelar sistemas "bypass", es necesario ejercer un control sobre estas ilegalidades que faciliten el manejo de información

al respecto, prevención, detección e intervención a los sistemas “bypass”. Para esto es necesario contar con herramientas tecnológicas mejores, o por lo menos igual de eficientes, que aquellas utilizadas para cometer los ilícitos.

Al mencionar ejercer un control se debe pensar en formas de prevenir y minimizar las posibilidades de “bypass”. Esto se puede lograr, primero, a través de medidas económicas que reduzcan el interés en esta práctica. Como se ha visto, el principal incentivo para un defraudador son las ganancias que puede tener en este ilícito. Se puede realizar el siguiente análisis:



	Costo de terminación por minuto en líneas fijas (ctvs.)								
	Legal					Oferta	Bypass		
Línea	**Internacional**		**CNT Fijo**	**Movi**	**Claro**	**Bypass**	**Ganancia**	**Ahorro %**	
Fija	0,09	0,12	0,01	0,26	0,18	0,08	0,07	13,42	30,68

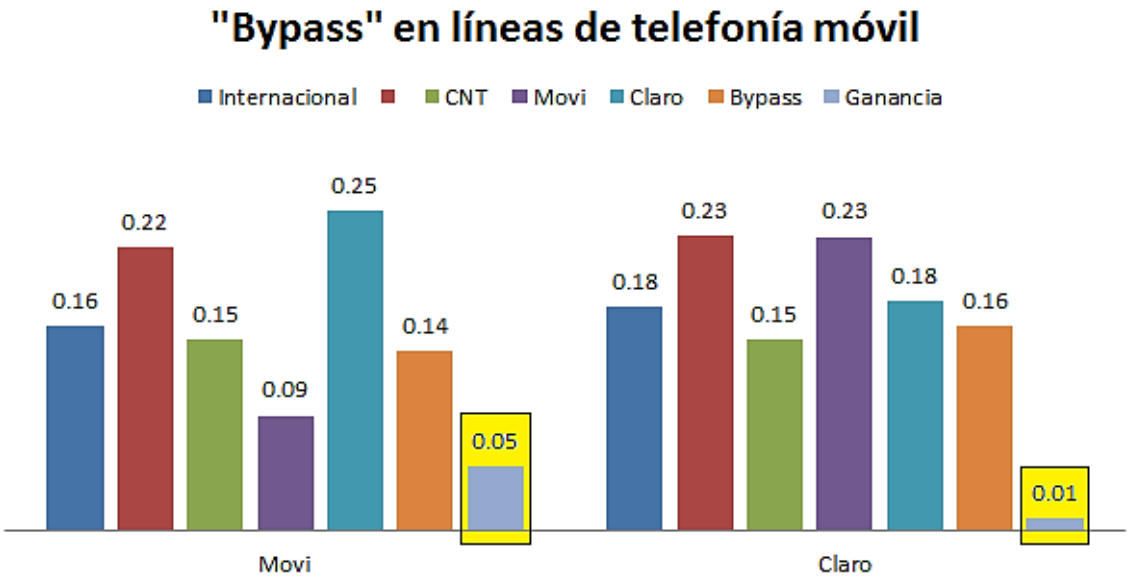
Figura 2.1. “Bypass” sobre telefonía fija [23,24]

En telefonía fija en el Ecuador, en base a la Figura 2.1, un “bypass” tiene una utilidad de alrededor de 7 ctvs. por minuto y un ahorro de alrededor de 13,42 % para los portadores internacionales. Esta utilidad es la diferencia entre la oferta del “bypass” y el costo de la llamada local utilizando líneas de telefonía fija.

[23]Los análisis se han realizado con los precios de las ofertas en los portales de venta de minutos IPsmarx y VOIP.ms, y precios publicados en las páginas web de las operadoras CNT, MOVISTAR y CLARO.

[24]En el análisis no se consideran promociones de las operadoras móviles, las cuales pueden aumentar la utilidad para los defraudadores según el caso.

En cuanto a telefonía móvil en el Ecuador, en base a la Figura 2.2, un “bypass” tiene una utilidad de alrededor de 5 ctvs. para Movistar y 1 ctv. para Claro por minuto y un ahorro de alrededor para el *carrier* internacional de 12,39 % y 20 % respectivamente, sin considerar promociones.



	Costo de terminación por minuto en líneas Movistar y Claro (ctvs.)								
	Legal					Oferta	Bypass		
Línea	**Internacional**		**CNT**	**Movi**	**Claro**	**Bypass**	**Ganancia**	**Ahorro %**	
Movistar	0,16	0,22	0,15	**0,09**	0,25	0,14	0,05	12,39	36,97
Claro	0,18	0,23	**0,15**	0,23	0,18	0,16	0,01	20,00	39,37

Figura 2.2. “Bypass” en líneas de telefonía móvil [25,26]

La utilidad que un defraudador percibe, como se puede ver, es alta debido a la diferencia entre costo de terminar una llamada internacional y una llamada local en las redes de las operadoras. Una forma de controlar este aspecto es evitar que el negocio sea rentable al defraudador a través del control de márgenes de terminación o el control de tarifas off-net. No obstante, este tipo de controles pueden generar pérdidas para las operadoras y están limitados por la situación del mercado, tanto local como internacional.

[25] Los análisis se han realizado con los precios de las ofertas en los portales de venta de minutos IPsmarx y VOIP.ms, y precios publicados en las páginas web de las operadoras CNT, MOVISTAR y CLARO.

[26] En el análisis no se consideran promociones de las operadoras móviles, las cuales pueden aumentar la utilidad para los defraudadores según el caso.

Otro aspecto muy interesante e importante en el control de sistemas “bypass” es el proceso de detección que tiene varias modalidades. Para la detección de sistemas “bypass” es necesario contar con herramientas tecnológicas adecuadas y, según la técnica que se utilice, la información necesaria por parte de las operadoras.

Las técnicas o métodos de detección pueden aplicarse manualmente o de forma automática utilizando software dedicado. Hasta la actualidad, los esfuerzos por mejorar los métodos de detección se han concentrado en dos técnicas principales y que pueden ser combinadas [21]:

1. Sistema de lazo cerrado o “*loop*”.
2. Perfilamiento telefónico o “*profiling*”.

2.1.1 SISTEMA DE LAZO CERRADO O “LOOP”

El método del sistema de lazo cerrado o “*loop*”, es uno de los más utilizados en Ecuador para combatir los sistemas “bypass”. Este método, al que en adelante llamaremos SISLAC, consiste en originar desde Ecuador una llamada de prueba desde el extranjero hacia un teléfono conocido en Ecuador, e identificar su ruta de ingreso. [10]

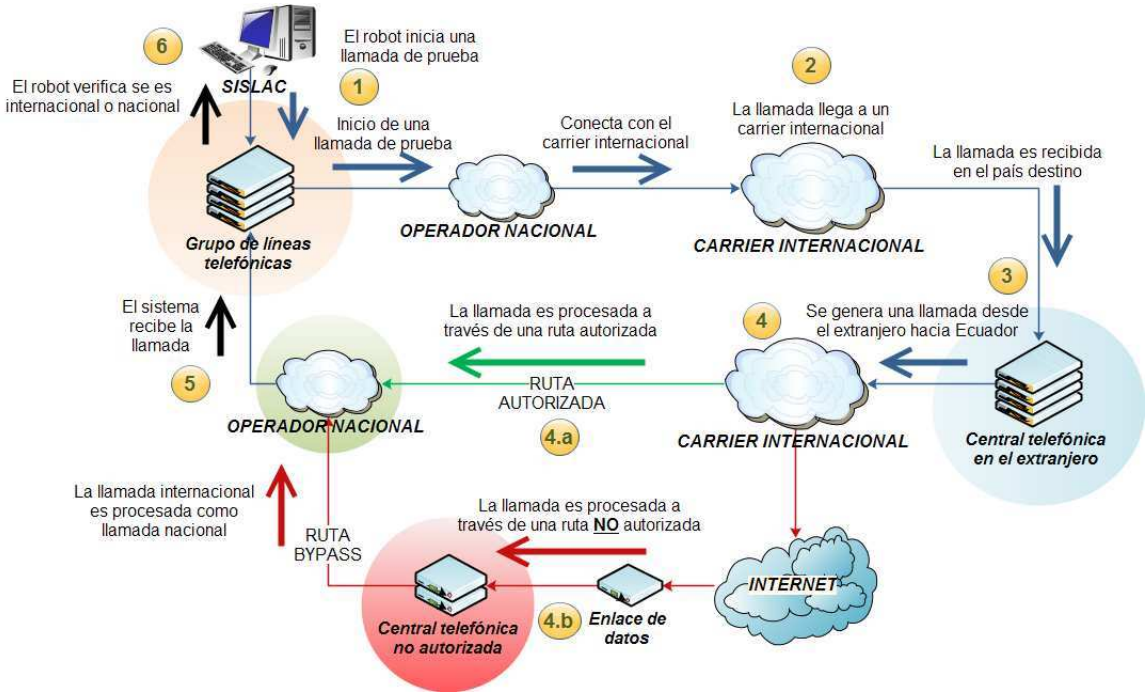


Figura 2.3. Funcionamiento de un sistema de lazo cerrado o “loop”

Como se observa en el diagrama de la Figura 2.3, el procedimiento para realizar una prueba de lazo cerrado es el siguiente: [10], [19], [20]

1. Se marca un número telefónico de una operadora en el país que se desee iniciar la prueba de lazo cerrado. La operadora puede ser un número de acceso de una tarjeta de telefonía pre-pagada de ese país o un enlace con una PBX. Por ejemplo, si se utiliza una tarjeta de telefonía pre-pagada comprada en los Estados Unidos, se marca el número de acceso de esa tarjeta en alguna ciudad de los Estados Unidos.

2. El operador local en Ecuador identifica y conecta la llamada con un *carrier* internacional, el mismo que se encargará de terminar la llamada en el destino especificado.

3. La operadora destino recibe y contesta la llamada de prueba en el país deseado. En este momento, si se trata de una llamada utilizando tarjetas de telefonía pre-pagada, la operadora solicita un código de acceso o PIN y un número de teléfono destino. Para realizar la llamada de prueba de lazo cerrado se marca un número destino en Ecuador.

4. La operadora en el extranjero identifica el destino de la llamada solicitada y la procesa hacia un *carrier* internacional para que sea direccionada hacia Ecuador.

    4. a. El *carrier* internacional coloca la llamada en una ruta autorizada, es decir, utiliza una conexión con el operador nacional que tiene asignado el número destino.

    4. b. El *carrier* internacional direcciona la llamada hacia una central telefónica no autorizada en el Ecuador. Esta central telefónica recibe la llamada a través de un enlace de datos, y la direcciona hacia el operador nacional que tiene asignado el número destino. Esta llamada internacional es percibida como llamada local.

5. La operadora nacional recibe la llamada de prueba iniciada en el extranjero y la procesa hacia el abonado asignado al número destino. La operadora retransmite el *Caller ID* recibido en desde el origen de la llamada.

6. El sistema de lazo cerrado recibe la llamada e identifica el *Caller ID* recibido. Si la llamada ingresó por una ruta autorizada, el *Caller ID* corresponderá a un código del *carrier* que proceso la llamada o al número que originó la llamada en Ecuador. Caso contrario, el sistema recibirá en el *Caller ID* un número telefónico local, indicativo de posible sistema “bypass”.

Este método puede ser utilizado junto a diferentes formas de llamada internacional, entre las cuales destacan dos utilizadas comúnmente en el Ecuador: a través de tarjetas de telefonía pre-pagada internacionales, y a través de portales web. [10]

2.1.1.1 SISLAC a través de tarjetas internacionales

En varios países es común la venta de tarjetas prepago para realizar llamadas internacionales de forma rápida y a bajo costo. Estas tarjetas operan a través de una central telefónica intermediaria a la cual el usuario debe conectarse antes de poder realizar la llamada internacional. Este sistema es aprovechado para generar llamadas de prueba internacionales. [10]

Figura 2.4. Tarjeta de telefonía pre-pagada de los Estados Unidos

En primer lugar se adquieren tarjetas de telefonía pre-pagada en países donde existe mayor índice de migración, como las de la Figura 2.4. Desde Ecuador se marca el número de acceso de la tarjeta según indican sus instrucciones, que generalmente vienen en el reverso de la tarjeta. A continuación se sigue las instrucciones del IVR de la tarjeta y se genera la llamada de prueba hacia Ecuador, al teléfono que va a recibir dicha llamada. [10]

El momento que ingresa la llamada, el teléfono recibe el identificador de llamante con lo cual se comprueba si la ruta utilizada para la llamada es legal o un "bypass". Este procedimiento se lo puede realizar utilizando un software diseñado particularmente para generar llamadas internacionales utilizando tarjetas pre-pagadas, lo cual aumenta la cantidad de pruebas que se realizan y se crea una base de datos de los números que se han registrado como fraudulentos. [10]

2.1.1.2 SISLAC a través de portales web

El mercado de tráfico se ha extendido a través del internet y es sencillo encontrar todo tipo de ofertas para realizar llamadas utilizando programas o portales en línea. Estos portales, además de ser sencillos de utilizar, permiten realizar llamadas a números telefónicos en distintos países a un costo determinado. Algunos programas que permiten realizar llamadas son SKYPE, Google Talk, etc.

Para realizar llamadas, en primer lugar se debe pagar a través de internet para tener un saldo que permita llamar al país deseado. Se accede al panel de marcación, dependiendo del portal o programa que se utilice, y se realiza la marcación hacia nuestro teléfono destino en Ecuador utilizando código de país, ciudad, etc. La llamada es originada a través de las redes que utiliza el portal o programa y una vez que ingresa al teléfono de pruebas, éste registra el identificador de llamante que puede ser legal o "bypass".

Figura 2.5. Logos de algunos portales de compra y venta de minutos

Otra posibilidad de realizar llamadas a través de Internet es utilizando portales y foros de compra y venta de minutos. En estos casos es necesario conectarse a un *carrier* internacional que enlace las redes que se van a conectar, de lo cual hablaremos más adelante. En los foros o portales donde proveedores ofrecen compra y venta de minutos, éstos permiten conectarse a su central para realizar llamadas internacionales a una tasa determinada. Véase la Figura 2.5.

Las centrales telefónicas que ofrecen este servicio permiten conexiones utilizando protocolos como SIP, IAX2 o H.323. Éstos son los protocolos más comunes, y para conectarse a ellos es necesario tener una central telefónica o un dispositivo de telefonía IP. De igual forma, se deben comprar minutos para realizar llamadas, las cuales serán destinadas al teléfono de pruebas para que este registre el identificador de llamante.

2.1.2 PERFILAMIENTO TELEFÓNICO O PROFILING

Otro método muy interesante para el seguimiento e identificación de un sistema "bypass" es el Perfilamiento telefónico o PROFILING. Este método consiste en el análisis del comportamiento de una línea telefónica, en cuanto a llamadas generadas y recibidas. [10]

Una línea telefónica tiene patrones de comportamiento definidos que dependen de las horas del día, día de la semana, feriados, etc. Estos patrones influyen en la utilización de la central telefónica, lo cual da un primer indicio de tráfico irregular. En el perfilamiento telefónico se analiza la cantidad de CDR's producidos por cada línea telefónica. En base a datos de llamadas como los minutos de consumo, horarios de uso y destino de llamadas, se puede determinar si el comportamiento de la línea es anormal, lo cual indica que puede estar siendo utilizada en un "bypass". Véase la Figura 2.6. [10]

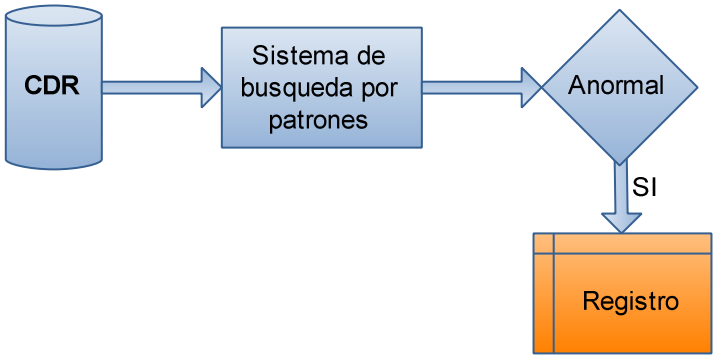


Figura 2.6. Estructura del sistema de perfilamiento telefónico

Esta técnica puede ser aplicada de forma automática o manual. En caso de ser manual, implica un trabajo enorme que comienza con el análisis del tráfico en centrales telefónicas. En aquellas centrales que registran tráfico elevado e

inusual, se procede a analizar las líneas que generan dicho tráfico y sus principales características como números destino, duración, etc.

Existen equipos y software que realiza este proceso de forma automática. Estos equipos reciben los CDRs, los analizan según sus criterios de comparación y reportan aquellas líneas que producen un tráfico inusual para que sean investigadas. Analizando detenidamente cada línea se puede determinar si estas líneas están siendo utilizadas en un posible sistema "bypass". Con esta información se notifica al organismo de control competente, en el Ecuador la Superintendencia de Telecomunicaciones, para dar paso al proceso de investigación, búsqueda y desarticulación del sistema no autorizado.

2.1.3 TÉCNICAS DE UBICACIÓN DE "BYPASS"

La detección de las líneas utilizadas en un sistema "bypass" es el primer paso en la investigación y desarticulación del sistema. Una vez identificado el origen del problema, se procede al análisis de la situación. Si se tratase de una línea asignada a un usuario conocido de un plan post-pago, lo cual es poco común, se verifican sus datos. [7]

Por lo general, para este tipo de ilícitos se utilizan líneas telefónicas pre-pagadas (telefonía celular), robo de líneas o fraude por suscripción. Esto permite al defraudador no involucrarse directamente con la operadora evitando que se lo identifique fácilmente. Mientras el "bypass" se encuentre operando generará pérdidas para la(s) operadora(s) involucrada(s), por lo cual es necesario entonces localizar el "bypass" para poder desmantelarlo. [21], [7], [10]

Cuando un sistema "bypass" utiliza líneas de una operadora de telefonía fija, es relativamente sencillo determinar su ubicación. Las operadoras de telefonía fija conocen los números asignados a cada distribuidor telefónico y sector, así como el lugar donde se encuentra instalado el bucle de abonado. Esto facilita el trabajo y permite conocer la ubicación rápidamente para proceder con las acciones legales. Sin embargo, en algunos casos las líneas se reparten en edificios u oficinas a través de cajetines, lo cual dificulta el trabajo de ubicación y da tiempo a los defraudadores para escapar. [10]

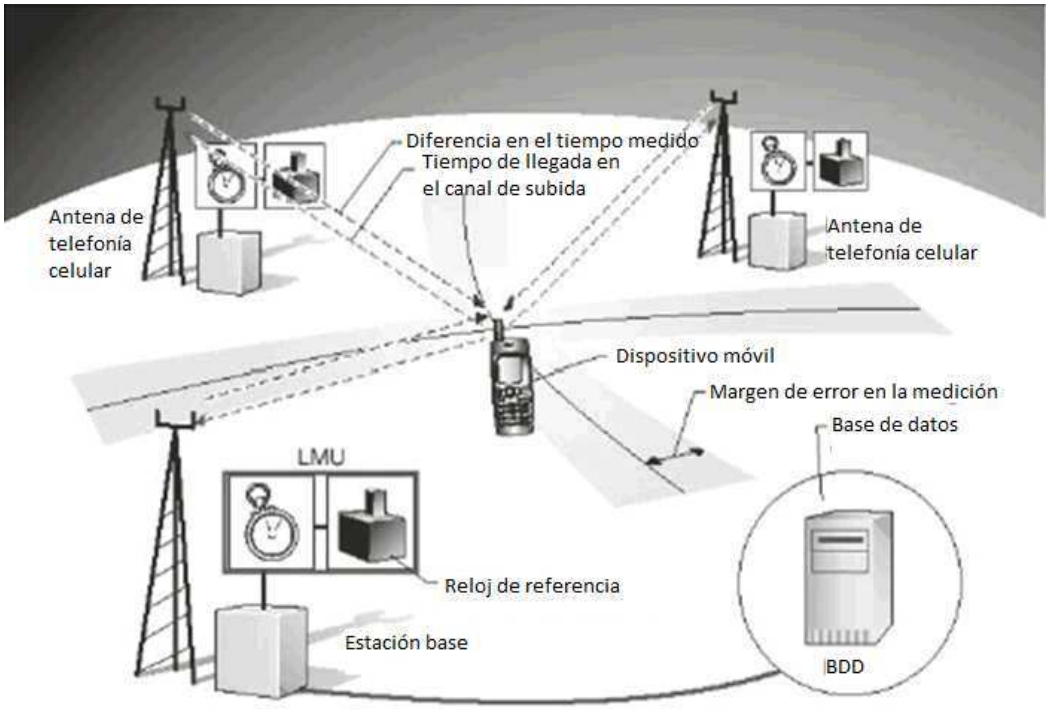


Figura 2.7. Esquema del sistema de localización por medición de tiempos. [7]

En el caso de los “bypass” que utilizan la red celular es más complicado el proceso de ubicación debido a que los equipos son inalámbricos y su ubicación más probable, en caso de detectar un “bypass”, es el área de cobertura de la BTS, es decir alrededor de 20 cuadras en zonas urbanas o algunos kilómetros en zonas rurales. Por esta razón, las técnicas utilizadas en telefonía celular para determinar la ubicación de una línea telefónica son más complejas y costosas. [10]

Adicionalmente GSM es una tecnología que utiliza saltos de frecuencia en su comunicación, por lo que la utilización de SIM BOX dificulta el proceso de seguimiento, ya que cada llamada es generada desde una línea y una frecuencia o canal diferente. Es importante mencionar que ninguna técnica es capaz de ubicar el lugar exacto del equipo móvil o la SIM BOX; en el mejor de los casos reducirá a unos cuantos metros la zona de ubicación más probable. Las técnicas más conocidas son: [7]

1. Potencia y tiempos de respuesta.- Esta técnica utiliza las características de potencia de la señal recibida del equipo y tiempo de retardo de los mensajes para calcular la distancia a la que probablemente se encuentra el

dispositivo. También se puede definir el ángulo de llegada de la señal a la BTS para reducir aún más la zona de ubicación más probable. En la Figura 2.7 se observa una representación de un sistema de localización por medición de tiempo UL-TOA[27] [46].

2. Triangulación.- Esta es quizás una de las técnicas más precisas para determinar la zona de ubicación más probable de un equipo. Esta técnica consiste en utilizar tres antenas, que pueden ser de la operadora o incluso satelitales, para trazar una recta en el sentido en que cada antena recibe la señal. Al cruzar las rectas se limitará una pequeña zona triangular, la cual corresponde a la zona más probable de ubicación del equipo. En algunos casos, y dependiendo de la topografía del lugar y la cantidad de edificios y objetos reflectores, puede reducir la zona más probable a unos cuantos metros [54].

3. Software.- Existen algunas aplicaciones que permiten conocer la posición geográfica de un dispositivo móvil. Esta tecnología es utilizada por algunas operadoras en el mundo para ofrecer un servicio de localización en caso de accidentes o emergencias. El limitante de esta técnica para los usos de este estudio es que estas aplicaciones necesitan de un teléfono celular, los cuales no se utilizan en sistemas “bypass”. [21]

En el Ecuador la Superintendencia de Telecomunicaciones, ente regulador, utiliza algunas de estas técnicas para dar seguimiento y localizar sistemas “bypass”. La SUPERTEL mantiene una relación muy cercana de cooperación con las operadoras de servicio telefónico en el Ecuador con el objetivo de trabajar coordinadamente en el control y detección de los delitos y fraudes en telecomunicaciones. [10]

2.2. COMBATE A LOS “BYPASS” EN EL ECUADOR [19], [20]

En el Ecuador, el organismo de control encargado del combate a los ilícitos en telecomunicaciones es la Superintendencia de Telecomunicaciones a través de la Dirección Nacional de Investigaciones Especiales en Telecomunicaciones. La

[27] Tiempo de llegada en el canal de subida o *Uplink Time of Arrival* por sus siglas en inglés.

Superintendencia trabaja de forma coordinada con las operadoras de telefonía desmantelando sistemas “bypass” y realizando acciones preventivas.

2.2.1 CANTIDAD DE “BYPASS” INTERVENIDOS EN LOS ÚLTIMOS AÑOS

De los datos facilitados por la Superintendencia acerca del número de sistemas telefónicos ilegales intervenidos durante los últimos cinco años, se observa en la Tabla 2.1 que suman un total de 129. [19], [20]

AÑO	CANTIDAD DE INTERVENCIONES REALIZADAS
2005	13
2006	18
2007	15
2008	17
2009	26
2010	40
TOTAL	129

Tabla 2.1. Intervenciones a sistemas de telefonía tipo “bypass” [19], [20]

Es importante resaltar la tendencia que se observa en el número de sistemas “bypass” en el Ecuador en los últimos años. Entre el 2005 y el 2010, el número de intervenciones realizadas se ha triplicado. Se puede observar con claridad la tendencia creciente que tienen este tipo de prácticas.

Del total de intervenciones realizadas por la SUPERTEL, aproximadamente el 31% se registraron el año pasado, es decir 40. Esta cifra es sumamente elevada y merece especial atención ya que revela que en promedio se interviene un sistema telefónico “bypass” cada 9 días.

En la Figura 2.8 se observa la tendencia que tiene el número de sistemas “bypass” intervenidos a través de los años. [19], [20]

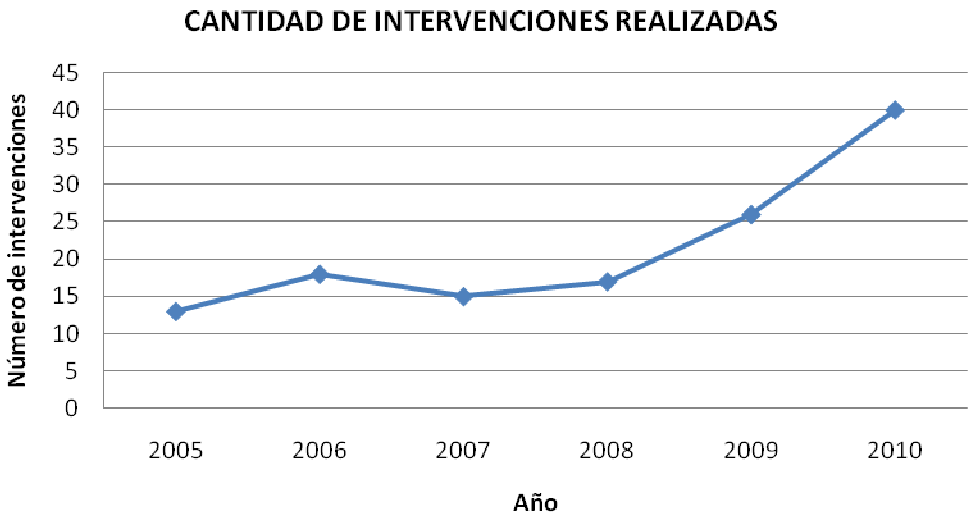


Figura 2.8. Número total de intervenciones realizadas por la SUPERTEL en los últimos 5 años [19], [20]

Considerando la inserción de "nuevas" empresas de telefonía en el mercado de las telecomunicaciones, es importante identificar el número de casos que se ha tenido en cada una de ellas. En la Tabla 2.2 se puede observar el listado de operadoras en donde se han realizado intervenciones y su número.

Operadora/Año	2005	2006	2007	2008	2009	2010	Total
Andinatel	2	1	3	2	3	6	35
Pacifictel	7	3	8				
Otecel	4	5	2	4	6	7	28
Conecel		9	1	10	6	20	46
Telecsa				1	3	6	10
Ecuadortelecom					6		6
Setel			1		2		3
Global Crossing						1	1
Total	13	18	15	17	26	40	129

Tabla 2.2. Número de intervenciones realizadas por operadora entre el 2005 al 2010 [19], [20]

De esta información, es importante destacar que la mayoría de “bypass” se han registrado en las operadoras de telefonía fija CNT y telefonía móvil Movistar (Otecel) y Claro (Conecel). Véase la Figura 2.9.

La operadora CNT tiene la particularidad de que desde el año 2008 opera como única empresa tras la unión de Andinatel (zona andina) y Pacifictel (zona costa). No obstante, se observa que entre los años 2005 y 2007 en la zona costa se realizó un mayor número de intervenciones que la zona andina. [19], [20]

En cuanto a las operadoras de telefonía fija se puede observar que hay una gran cantidad de sistemas intervenidos. Esto se debe principalmente a la aparente seguridad que brinda la telefonía móvil ya que es fácil asumir que las líneas de telefonía celular son difíciles de ubicar geográficamente, lo cual no necesariamente es cierto. [19], [20]

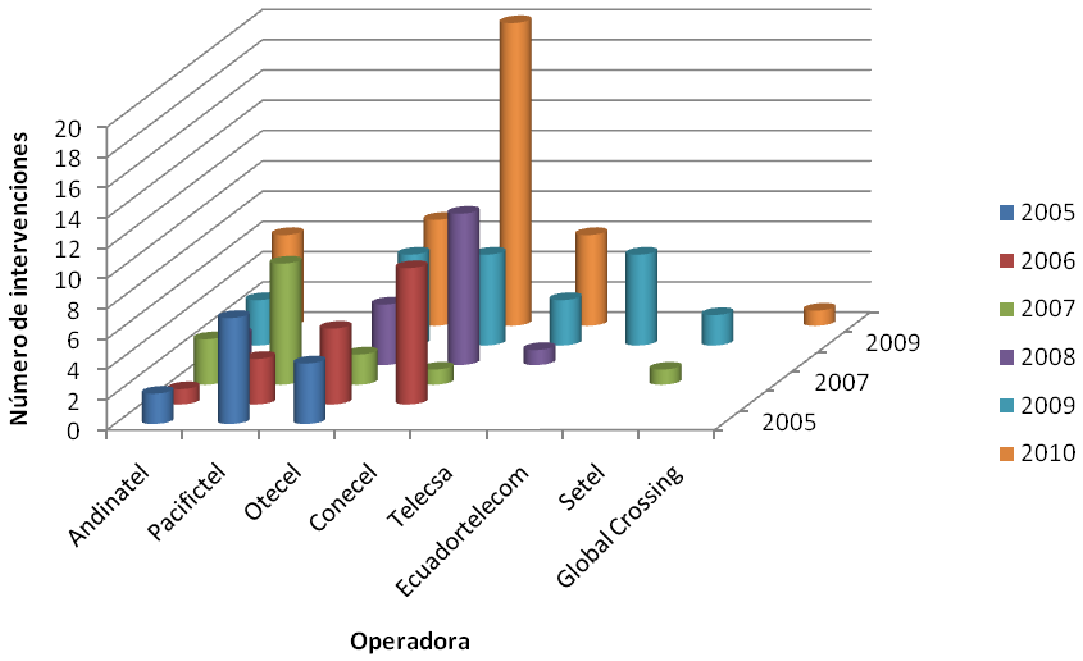


Figura 2.9. Número de intervenciones realizadas por operadora. [19], [20]

Como se ha visto en apartados anteriores, existen diferentes técnicas para identificar posibles sistemas “bypass”, las cuales se combinan con técnicas de ubicación geográfica que pueden resultar incluso más eficientes que las utilizadas en la telefonía fija.

2.2.2 MODALIDADES DE OPERACIÓN DE LOS "BYPASS" EN EL ECUADOR

Para la SUPERTEL, la modalidad de operación de un sistema "bypass" está definida por 3 elementos que forman parte de dichos sistemas: [19], [20]

1. Enlace de datos.- Utilizado para establecer la comunicación con el origen del tráfico internacional.
2. Equipos de telecomunicaciones.- Utilizados para procesar el tráfico telefónico y direccionarlo a la PSTN.
3. Líneas telefónicas.- Utilizadas para terminar de forma no autorizada en la red pública las llamadas originadas en el exterior.

A través de los años y con la aparición de nuevas tecnologías, estos elementos descritos han cambiado. Este hecho ha repercutido en las modalidades que se utilizan actualmente en la implementación de estos sistemas. [19], [20]

Con respecto a los enlaces digitales utilizados, se puede mencionar los siguientes casos: [19], [20]

- Enlaces satelitales.
- Enlaces dedicados mediante líneas de cobre.
- Enlaces por fibra óptica.
- Enlaces "*spread spectrum*", punto - multipunto con el uso de antenas omnidireccionales.
- Enlaces sobre redes HFC.
- Enlaces digitales inalámbricos instalados clandestinamente, como extensión de un enlace autorizado.
- Enlaces digitales con tecnología WiMAX.

Los equipos de telecomunicaciones que se han utilizado en los diferentes casos son los siguientes: [19], [20]

- Equipos para voz sobre "*Frame Relay*".
- Concentradores telefónicos VoIP.
- Gateway de voz para redes fijas.
- Gateway de voz para redes móviles.
- Gateway de voz GSM.
- "SIM BOX" para almacenamiento de tarjetas SIM.

Finalmente, en cuando a líneas telefónicas utilizadas para terminar las llamadas internacionales se han utilizado los siguientes tipos: [19], [20]

- Líneas de telefonía fija.
- Líneas telefónicas RDSI[28].
- Líneas de telefonía móvil.
- Líneas sobre redes HFC[29].

Adicionalmente, el funcionamiento de un sistema "bypass" está determinado por la forma en que este sea estructurado. Combinando los elementos descritos su puede tener una variedad de sistemas "bypass" con operatividad tecnológica diferente, y que presentan diversos retos para su investigación.

Un ejemplo bastante claro es el uso de concentradores telefónicos VoIP que han ganado popularidad por sus alternativas en software. [19], [20]

2.2.3 PERJUICIO ECONÓMICO

Los fraudes a los sistemas telefónicos están motivados principalmente por el aspecto económico, como lo están los fraudes en general. El campo de las telecomunicaciones involucra gran cantidad de dinero por lo que este tipo de fraude provoca perjuicios que suman millones de dólares.

[28] Acrónimo de Red Digital de Servicios Integrados, es una red que brinda conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios.
[29] Acrónimo de Híbrido de Fibra y Coaxial, se refiere a una red que incorpora tanto fibra óptica como cable coaxial para crear una red de banda ancha.

Como se puede observar en la Tabla 2.3 que contiene la información entregada por la Superintendencia, el combate a los sistemas “bypass” ha significado evitar un perjuicio que supera los 68 millones de dólares entre los últimos 5 años.

AÑO	MONTO ESTIMADO QUE SE EVITÓ PERDER POR ACCIONES DE LA SUPERINTENDENCIA (USD)
2005	3.486.033,00
2006	17.609.200,00
2007	8.801.691,00
2008	11.508.109,00
2009	11.646.597,00
2010	15.599.168,00
TOTAL	68.650.798,00

Tabla 2.3. Monto que la SUPERTEL evitó perder en los últimos 5 años. [19], [20]

Esta cifra deja muy en claro la importancia económica que representa este tipo de fraude para las empresas privadas y estatales, considerando que las más afectadas son CNT, Movistar y Claro.

Figura 2.10. Monto de la pérdida evitada por la Superintendencia. [19], [20]

El perjuicio estimado que se ha evitado gracias a la labor de la SUPERTEL se refiere al monto económico que las intervenciones realizadas evitaron que se pierdan. En la Figura 2.10 se observa un diagrama de barras que ilustra estos valores.

En el año 2006 se presentó un incremento significativo en el perjuicio evitado por la Superintendencia a través de sus investigaciones e intervenciones. En adelante, a partir del 2007 donde el perjuicio evitado disminuyó significativamente frente al 2006, se observa un incremento cada año, el cual concuerda con el comportamiento creciente del número de sistemas “bypass” intervenidos en los últimos años.

Estas cifras, sumadas al creciente número de “bypass” en los últimos años, reflejan la necesidad de mantener un combate efectivo a este tipo de delitos. Para esto es necesario contar con herramientas especializadas que contribuyan a agilizar los procedimientos de identificación y ubicación de estos sistemas.

2.3 APLICACIÓN DEL SISTEMA DE LAZO CERRADO [19], [20], [26]

El sistema de lazo cerrado, como se ha visto, es una herramienta para combatir el fraude tipo “bypass”; sin embargo, en adición al desarrollo técnico es importante estudiar el número de llamadas internacionales al Ecuador entrantes durante cada año para estimar una cantidad adecuada de pruebas necesarias.

2.3.1 TRÁFICO TELEFÓNICO INTERNACIONAL EN EL ECUADOR

La SUPERTEL como organismo de control y para el trabajo de prevención y combate a los ilícitos en telecomunicaciones tiene un registro anual de la cantidad de llamadas internacionales entrantes y salientes, y su duración total. Este registro se encuentra disponible desde el año 2008 hasta la actualidad.

De acuerdo a los datos de la SUPERTEL, durante el año 2008 se registraron la siguiente cantidad de llamadas internacionales entrantes y salientes detalladas en las Tablas 2.4, 2.5 y 2.6:

	FIJO		MÓVIL		TOTAL
MES	Entrantes	Salientes	Entrantes	Salientes	
Enero	8.052.232	1.778.848	9.176.578	8.153.018	27.160.676
Febrero	7.593.377	1.672.309	8.699.876	7.575.160	25.540.722
Marzo	8.246.924	1.783.540	9.414.855	8.384.766	27.830.085
Abril	7.951.044	1.845.955	8.916.073	8.045.966	26.759.038
Mayo	8.527.652	1.909.961	9.353.211	8.747.405	28.538.229
Junio	8.058.843	1.821.071	8.777.611	8.681.107	27.338.631
Julio	8.112.773	1.959.556	9.008.880	9.144.565	28.225.774
Agosto	7.817.081	1.894.177	8.983.948	9.231.616	27.926.822
Septiembre	8.590.082	1.893.299	9.076.370	9.038.578	28.598.329
Octubre	7.638.837	1.882.745	8.935.229	9.145.392	27.602.203
Noviembre	7.114.639	1.782.103	8.720.264	8.949.534	26.566.539
Diciembre	7.949.922	1.966.515	9.382.794	10.408.988	29.708.218
TOTAL	95.653.405	22.190.077	108.445.689	105.506.095	331.795.266

Tabla 2.4. Cantidad de llamadas internacionales durante el 2008 [19], [20]

Durante el año 2009 se registraron la siguiente cantidad de llamadas internacionales entrantes y salientes:

	FIJO		MÓVIL		TOTAL
	Entrante	Saliente	Entrante	Saliente	
Enero	7.608.892	2.147.957	9.292.739	9.114.115	28.163.704
Febrero	6.505.339	1.967.925	8.285.783	8.170.138	24.929.184
Marzo	7.143.372	2.143.679	9.292.862	9.358.787	27.938.700
Abril	6.789.761	2.182.677	8.660.022	8.364.776	25.997.236
Mayo	7.208.128	2.116.638	9.223.165	9.043.051	27.590.982
Junio	6.827.401	2.070.180	8.734.041	8.954.814	26.586.436

	FIJO		MÓVIL		TOTAL
Julio	6.940.931	2.073.442	9.067.490	9.066.421	27.148.285
Agosto	6.847.198	1.974.117	9.341.121	9.176.969	27.339.405
Septiembre	6.648.614	1.866.281	8.824.480	8.896.870	26.236.245
Octubre	6.376.912	1.853.181	9.036.220	9.234.764	26.501.076
Noviembre	6.042.046	1.706.176	8.697.927	9.148.850	25.594.999
Diciembre	6.915.796	1.899.022	9.736.097	10.962.135	29.513.050
TOTAL	81.854.390	24.001.274	108.191.947	109.491.690	323.539.301

Tabla 2.5. Cantidad de llamadas internacionales durante el 2009 [19], [20]

Durante el año 2010 se registraron la siguiente cantidad de llamadas internacionales entrantes y salientes:

	FIJO		MÓVIL		TOTAL
	Entrante	**Saliente**	**Entrante**	**Saliente**	
Enero	6.562.262	1.774.285	9.154.521	9.561.652	27.052.720
Febrero	5.861.967	1.650.918	8.322.706	8.495.643	24.331.234
Marzo	6.186.757	1.893.037	9.048.612	9.370.658	26.499.064
Abril	5.918.315	1.712.103	8.575.851	8.224.881	24.431.151
Mayo	6.809.632	1.828.784	8.924.878	8.928.080	26.491.374
Junio	6.240.964	1.741.067	8.256.838	8.505.731	24.744.600
Julio	6.193.019	1.818.788	8.819.622	8.876.139	25.707.568
Agosto	6.847.760	1.849.003	9.367.464	9.330.978	27.395.205
Septiembre	6.449.070	1.839.111	8.951.780	8.188.113	25.428.074
Octubre	6.430.888	1.814.499	8.941.469	8.450.028	25.636.884
Noviembre	6.155.770	1.739.177	8.424.814	9.264.548	25.584.309
Diciembre	6.876.781	1.896.092	9.496.302	10.284.798	28.553.973
TOTAL	76.533.186	21.556.863	106.284.857	107.481.249	311.856.155

Tabla 2.6. Cantidad de llamadas internacionales durante el 2010 [19], [20]

La implementación de un sistema de lazo tiene estrecha relación con esta información. Como se observa en la Figura 2.11, la cantidad de llamadas entrantes en conjunto supera la cantidad de llamadas salientes, lo que indica que la mayor cantidad de tráfico internacional es entrante. En el caso de la telefonía móvil, este fenómeno tiene relación con el menor costo de llamada y las promociones que constantemente las operadoras ofrecen.

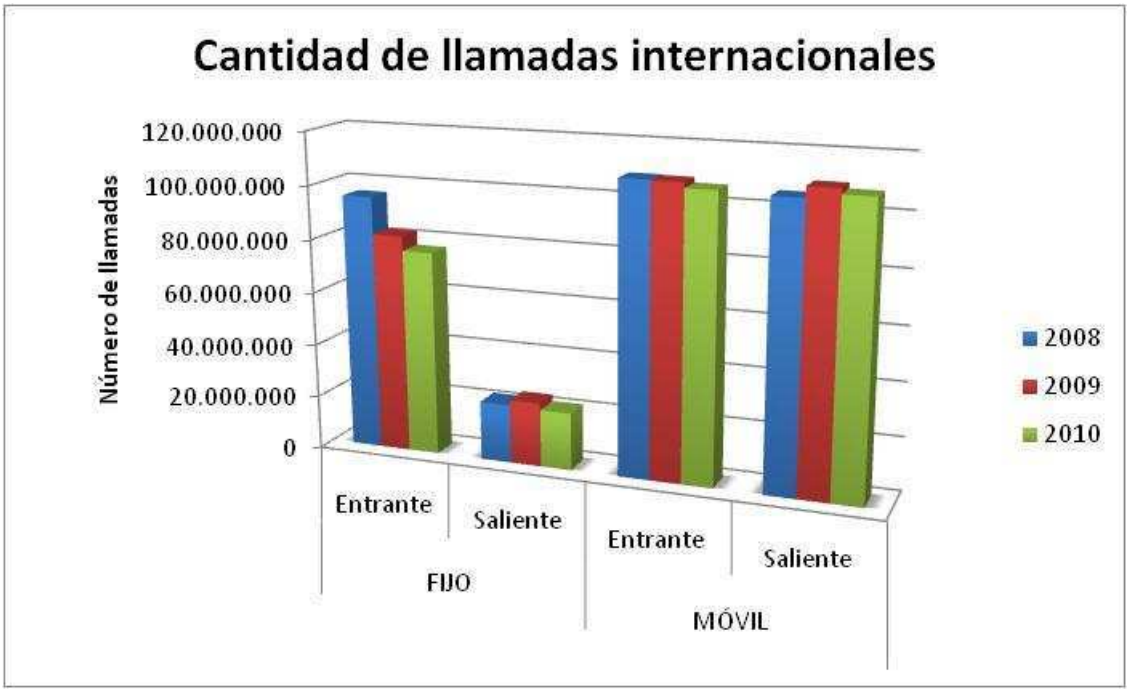


Figura 2.11. Cantidad de llamadas internacionales (2008 – 2010) [19], [20]

Por otro lado, la duración de estas llamadas tiene un comportamiento diferente. Como se puede observar en la Figura 2.12, la duración de llamadas entrantes es mucho mayor a la duración de las llamadas salientes.

Este fenómeno corresponde a la forma en que la gente utiliza este servicio. Es mucho más común que en una llamada recibida desde el extranjero en el Ecuador, la gente hable más tiempo. Por lo general, para llamar a países de Sudamérica se utilizan medios como las tarjetas de telefonía pre-pagada, los cuales resultan más económicos y permiten hablar por mayor tiempo.

Esta es una de las razones por las cuales este tipo de medios representa un posible foco de sistemas “bypass”, ya que por sus bajos precios necesitan puntos de conexión que ofrezcan menor costo, pudiendo ser legales o no.

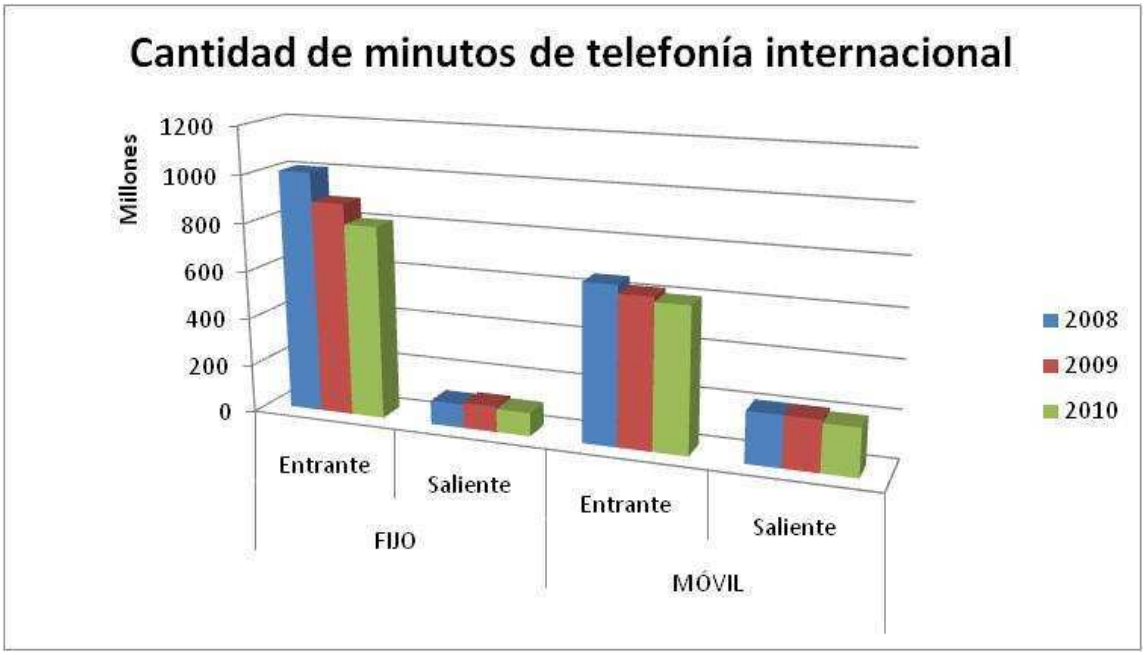


Figura 2.12. Cantidad de minutos de telefonía internacional (2008 – 2010) [19]

Para el portador de tráfico telefónico internacional en el extranjero resulta transparente el camino a través del cual accede a la red pública nacional; y, en la práctica, el delito tiene una jurisdicción estrictamente nacional, ya que el portador que envía el tráfico desde el extranjero está pagando por la terminación, pese a que ésta no sea autorizada.

2.3.2 APLICACIÓN DEL SISTEMA DE LAZO CERRADO

Implementar y ejecutar un sistema para pruebas de lazo cerrado implica, además del desarrollo técnico, un estudio sobre la cantidad de llamadas internacionales para determinar el número de pruebas mínimo que se debe realizar durante el año para tener resultados confiables. El presente estudio hace énfasis en las llamadas entrantes ya que el tipo de “bypass” que el sistema de lazo cerrado combate son de tráfico telefónico entrante.

La cantidad de tráfico telefónico internacional que ingresa al Ecuador está relacionada con la época del año. Como se observa en la Figura 2.13, durante ciertos meses (enero, mayo, septiembre, y diciembre) hay un incremento de las llamadas internacionales entrantes. Esto generalmente coincide con fechas festivas como navidad, día de las madres, o año nuevo, entre otras.

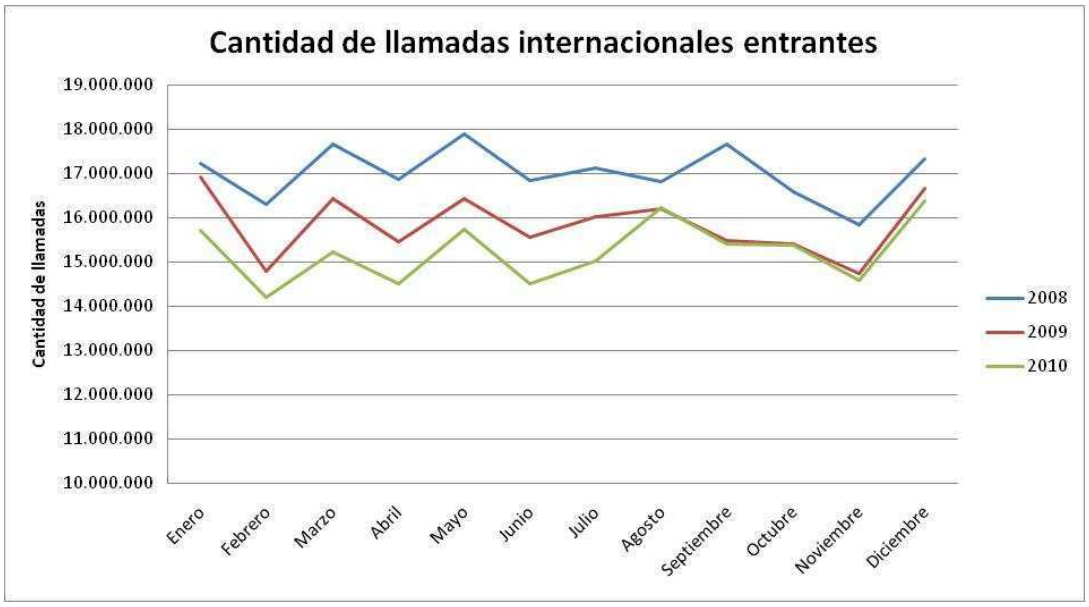


Figura 2.13. Comportamiento del tráfico telefónico durante el año

En la Tabla 2.7 se observa la cantidad total de llamadas por año del 2008 al 2010. Es entonces importante definir la época del año como un primer parámetro de investigación, es decir, en meses específicos se debe concentrar una mayor cantidad de pruebas.

Año	Cantidad de llamadas
2008	204101102
2009	190.048346
2010	182820053
Promedio:	192323167

Tabla 2.7. Cantidad de llamadas entrantes anuales

Para determinar un número mínimo de pruebas a realizarse, es posible utilizar herramientas estadísticas como el cálculo del tamaño de una muestra probabilística. Este teorema permite definir la cantidad de muestras que se debe tomar de un universo de llamadas para que ésta sea confiable. Este teorema se basa en análisis probabilísticos, y está determinado por la siguiente ecuación: [26]

$$n = \frac{Z^2 pqN}{Ne^2 + Z^2 pq}$$

Donde:

- n: Tamaño de la muestra. Número de muestras a tomar.
- Z: Nivel de confianza. Representa el grado de exactitud de la información recogida de la muestra. Típicamente se considera un error del 5%, es decir un nivel de confianza del 95% que equivale a Z = 1,96.
- p/q: Variabilidad positiva y negativa. Son variables que representan la desviación en la medición. Para análisis estándar se utiliza 0,5 para ambas.
- N: Tamaño de la población. Cantidad total de llamadas entrantes.
- e: Precisión o error. Porcentaje de error máximo de la muestra. El error típico utilizado es del 5%.

Al aplicar esta ecuación, se determina una cantidad de llamadas en las cuales se contiene la mayor cantidad de información del universo de llamadas. En este grupo de llamadas de muestra existirá un porcentaje de llamadas que ingresaron a través de una ruta no autorizada, porcentaje que a su vez es muy cercano al presente en la totalidad de la muestra. [26]

Considerando una variabilidad máxima, donde p = q = 0,5; un nivel de confianza del 95%, es decir Z = 1,96; y un error máximo del 5%, es decir 0.05; se tienen los siguientes resultados: [26]

$$n = \frac{(1.96)^2 x\ 0.5\ x\ 0.5\ x\ N}{N\ x\ (0.05)^2 + (1.96)^2 x\ 0.5\ x\ 0.5}$$

$$n = \frac{0{,}9604N}{0.0025N + 0.9604}$$

En cuanto al tamaño de la muestra, como se observa en la Tabla 2.7, en el año 2008 existe la mayor cantidad de llamadas, seguida del 2009 y el 2010 respectivamente. Para el caso del menor número de llamadas, en el 2010, se tienen los siguientes resultados:

$$n = \frac{182820053\ x\ 0.9604}{182820053\ x\ 0.0025 + 0.9604}$$

$$n = \frac{175580378{,}9012}{457051{,}0929}$$

$$n = 384{,}1591 \cong 385\ llamadas$$

Para el caso del promedio del número de llamadas durante los 3 últimos años, se tienen los siguientes resultados:

$$n = \frac{192323167\ x\ 0.9604}{192323167\ x\ 0.0025 + 0.9604}$$

$$n = \frac{184707169{,}5868}{480808{,}8779}$$

$$n = 384{,}1592 \cong 385\ llamadas$$

El valor obtenido del cálculo de la muestra coincide con el criterio de muestra para un universo de datos extremadamente grande (considerado como infinito), donde se utiliza la fórmula: [26]

$$n = \frac{Z^2 pq}{e^2}$$

Aplicando los mismos valores considerados, se tiene:

$$n = \frac{(1.96)^2 x\ 0.5\ x\ 0.5}{(0.05)^2}$$

$$n = \frac{0.9604}{0.0025}$$

$$n = 384.16 \cong 385\ llamadas$$

Como se puede ver, para una confiabilidad del 95% en la muestra, dada la gran cantidad de llamadas internacionales entrantes que se realizan anualmente, es necesario únicamente verificar 385 de ellas a fin de obtener resultados confiables.

2.4 MERCADO MUNDIAL DE LAS TELECOMUNICACIONES [17]

Al hablar del mercado de las telecomunicaciones se tiende a hacer referencia a la situación actual de número de usuarios, servicios, proveedores, capacidades, consumo, etc. Eso es en la práctica el mercado, la oferta y demanda de servicios

de telecomunicaciones y en rasgos generales, cada año crece la demanda y los servicios convergen reduciendo costos y simplificando las redes y las comunicaciones. Véase la Figura 2.14. [63]

Para el propósito de este trabajo no es necesario detenerse a analizar la situación del mercado mundial, lo cual por cierto merecería un estudio independiente para recoger las perspectivas económicas, jurídicas y sociales de su situación actual. El presente análisis se concentra en aspectos más técnicos para comprender como funciona el mercado para proveedores y usuarios.

La importancia de este tema se centra en la utilidad que dan los sistemas no autorizados a este mercado. En sus inicios, la bolsa de tráfico corría sobre las mesas de negociación de las operadoras. Hoy en día la bolsa de tráfico se corre sobre Internet y muchas veces la relación entre un proveedor y sus clientes es impersonal, lo que facilita a los sistemas no autorizados ofrecer el servicio de terminación. [63]

Todos los mercados de telecomunicaciones actualmente se manejan a través de IP y VoIP. Existe variedad en cuanto a portadores internacionales y mercados de compra o venta de minutos. Uno de los mercados más grandes es ARBINET. ARBINET es una empresa que ofrece servicios de portador y compra/venta de minutos en un portal bastante interactivo, con presencia en prácticamente todo el mundo y con las empresas de telecomunicaciones más reconocidas.

Figura 2.14. Presencia de ARBINET en el mundo [29]

Hay varias empresas en el mercado, que como ARBINET ofrecen un lugar para negociar la compra y venta de minutos, así como servicios de portador. Incluso en Internet, se pueden encontrar foros de discusión con personas o empresas que realizan ofertas abiertamente de terminación en determinados países. Estos pequeños mercados pueden ser utilizados por quienes han implementado un sistema no autorizado para ofrecer el servicio. [29]

Antes de mencionar algunos de los portales para la negociación de tráfico telefónico es importante revisar aquellas medidas que permiten determinar la calidad de una red y son importantes conocer. Como en todo producto o servicio que se desea ofrecer la calidad es muy importante y como una referencia de calidad de las redes telefónicas se utilizan medidas como el ASR o el ACD.

2.4.1 MEDIDAS DE CALIDAD

No se puede hablar de un mercado de tráfico sin hacer énfasis de la calidad de las redes de los proveedores. En el mercado de tráfico se negocia la venta y compra de minutos de telefonía tomando como referencia los niveles de calidad que cada proveedor ofrece con su red. Estos niveles marcan la diferencia entre proveedores con similares ofertas y justifican incrementos o disminución del costo entre otras ofertas. [17]

Sin ser distante a las regulaciones de la UIT-T en este tema, en el mercado de tráfico intervienen tres términos de medidas de calidad: ASR[30] o tasa de tomas con respuesta, PGAD[31] o demora de respuesta después de la puerta de enlace y ALOC[32] o duración media de la conversación. [17]

2.4.1.1 Tasa de tomas con respuesta (ASR)

Interpretado por la UIT como uno de los valores de medida más importantes con que se mide la calidad de una red. Este valor ha sido utilizado por mucho tiempo en las negociaciones de conexión para tráfico telefónico. La norma E.425 de la UIT-T lo define como “la relación entre el número de tomas que dan lugar a una

[30]Acrónimo de Relación de Llamadas Conectadas o *Answer Seizure Ratio* por sus siglas en inglés.
[31]Acrónimo de Demora de Respuesta Después de la Puerta de Enlace o*Post Gateway Answer Delay* por sus siglas en inglés.
[32]Acrónimo de duración media de la Conversación o *Average Length Of Conversation* por sus siglas en inglés.

señal de respuesta y el número total de tomas. Constituye una medición directa de la eficacia del servicio ofrecido y se expresa generalmente como un porcentaje, de la siguiente manera":

$$ASR = \frac{Tomas\ que\ dan\ como\ resultado\ una\ señal\ de\ respuesta}{Número\ total\ de\ tomas} x100$$

En otros términos, es la relación que existe entre los intentos de llamada y las llamadas completadas. Esta proporción por obvias razones depende de muchos factores, de los cuales algunos son propios de la red y otros ajenos a ella. Entre las causas propias de la red están la señalización que utiliza y la congestión de la red más allá de la red internacional.

Por otro lado el ASR también depende, entre otros, de la frecuencia con que la línea del abonado final se encuentra ocupada, la manera de efectuar la marcación, y la penetración de dispositivos de respuesta automática, que afecta a la frecuencia con que se producen tonos de ausencia de respuesta. En general, el comportamiento del cliente afecta a esta medida, aunque no sea una característica de la red.

Los ASR representan una herramienta que se utiliza para comparar la calidad entre diferentes rutas hacia destinos comunes y la diferencia entre uno u otro ASR se debe atribuir a las redes que intervienen.

Los datos para calcular el ASR de una ruta se toman de los CDR, y en el caso de redes internacionales, se utilizan la toma de un troncal internacional. Es muy común que aquellas ofertas con un ASR muy bajo se traten de sistemas "bypass" en el país de destino.

2.4.1.2 Demora de respuesta después de la puerta de enlace (PGAD)

Otro factor que se debe analizar para medir la calidad de múltiples rutas hacia un mismo destino es el tiempo de establecimiento de la llamada, para el cual se utiliza la unidad PGAD o demora de respuesta después del Gateway. Este factor es una forma económica de analizar la calidad de las rutas y el usuario lo percibe con facilidad ya que es el tiempo que debe esperar el usuario para realizar una llamada, es decir la rapidez con que responde una red.

La Recomendación E.431 define tres intervalos de tiempo pertinentes: demora de la señal de invitación a marcar, demora después de marcar y demora de liberación de la llamada. El intervalo de demora después de marcar (PDD) da una idea del tiempo que necesita una red para realizar la interconexión a su destino luego de que el usuario ha marcado el número destino. [17]

La UIT-T define textualmente al PGAD como “el intervalo de tiempo entre la toma del circuito internacional y la recepción de la supervisión de la contestación del abonado”, es decir el tiempo desde que la llamada ingresa a una troncal internacional y es recibida por el abonado destino. En la Figura 2.15 se puede apreciar un diagrama de la duración del intervalo del PGAD.

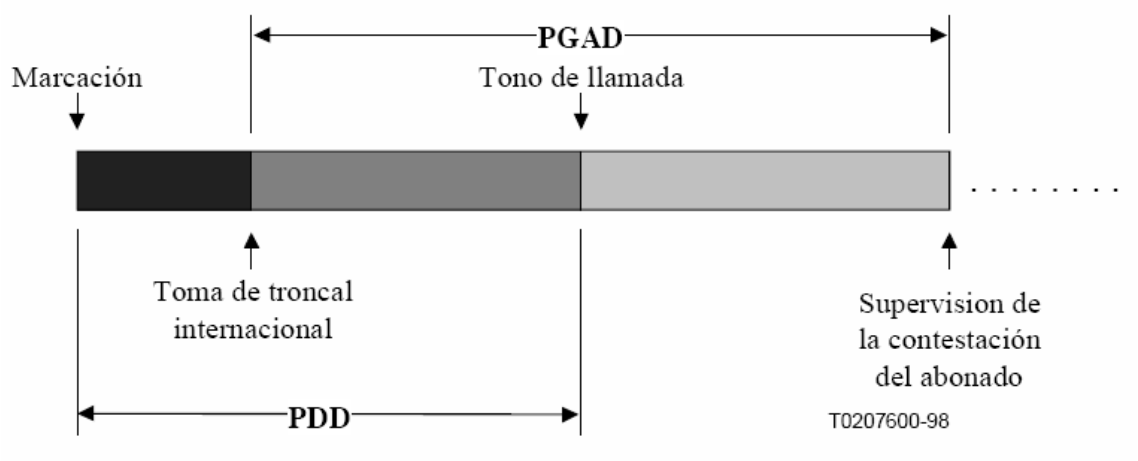


Figura 2.15. Esquema representativo del intervalo PGAD [17]

Al PGAD se lo puede dividir en dos pequeños intervalos. El primero que depende de la calidad de la red es el tiempo entre la toma de la troncal y la primera respuesta de la red.

El segundo, la contestación del abonado, depende del usuario. El PGAD observado sobre una sola ruta no resulta mayormente útil. Al comparar dos o más rutas con muestras de datos amplias y cuidadosamente seleccionadas, no se debe observar una diferencia significativa dado el comportamiento del cliente por lo que una variación significativa puede atribuirse al comportamiento de las redes particulares. [17]

2.4.1.3 Duración media de la conversación (ALOC)

La duración media de la conversación (ALOC), también conocida como duración media de la llamada (ACD[33]), es una unidad que mide el tiempo promedio de duración de una llamada por múltiples rutas hacia un mismo destino. Al comparar varias rutas hacia un mismo destino, donde que cada ruta lleva una porción del tren de tráfico común, lo normal es que la duración de una llamada sea similar y cualquier cambio en esta duración merece un análisis de las causas en la red.

La ALOC se mide solo en llamadas completadas se debe medir desde que el usuario destino contesta el teléfono (supervisión de la contestación) hasta que se termina la llamada. En caso de que no se pueda tomar el tiempo desde que el destinatario contesta la llamada, se lo puede tomar desde el acceso de la llamada a la troncal internacional, aunque el tiempo que demore el usuario en contestar generará un error. Sin embargo, dado que normalmente el tiempo que dura una conversación es por mucho mayor al tiempo del establecimiento de la llamada, este error no es significativo. Todas las rutas deben medirse de la misma manera.

Varios factores pueden afectar el ALOC. Un aumento en la cantidad de fallos de las transmisiones generará una disminución del ALOC. De igual manera, equipos de retransmisión o compresión pueden influir en la calidad de voz lo cual puede afectar al ALOC. De igual forma, la señalización que se utilice y los cambios en los planes de numeración pueden generar llamadas de menor duración, afectando al ALOC. [17]

Otro factor que puede influir disminuyendo el ALOC es una ruta donde se produce un nivel mayor de cortes de llamadas provocados por la red, lo cual generará un ALOC menor a la referencia. Este es un factor de calidad difícil de controlar en el caso de los sistemas “bypass” debido a que al ser detectados, muchos operadores cortan el tráfico a través de sus líneas, provocando cortes en las llamadas. Hay otros factores adicionales, distintos de los ya indicados, que podrían hacer que difieran las ALOC de dos rutas. [17]

[33]Acrónimo de Promedio de Duración de Llamada o *Average Call Duration* por sus siglas en inglés.

2.4.2 PARTICULARIDADES DEL MERCADO

La “convergencia” es un término que ha ganado popularidad en los últimos años. Consiguiendo lo que probablemente fue en sueño para muchas personas hace varios años, y una utopía para otras, la convergencia lleva al límite el desarrollo tecnológico a través de la unificación de servicios de telecomunicaciones.

Hasta hace poco, las redes de información fueron consideradas independientes de servicios de telefonía y televisión o video. Sin embargo, la convergencia que poco a poco comenzamos a vivir rompe esos paradigmas tradicionales para ofrecer un mercado de servicios unificados, capaz de satisfacer las necesidades de los usuarios con una sola plataforma que brinda servicios de telefonía, video y datos.

En este punto es necesario volver a analizar lo que hasta hoy se ha considerado fraude en telecomunicaciones. El mercado de telefonía ha migrado al uso de tecnologías IP, lo cual facilita su transporte a través de Internet. Es sencillo encapsular voz o video sobre IP y enviarlo como paquetes de datos a través de un enlace a Internet, por lo cual cabe cuestionarse si eso se puede considerar fraude.

En Internet la gran mayoría de portales para compra o venta de servicios de telefonía utilizan protocolos de VoIP como SIP, IAX o H.323. Esto mejora la calidad en los servicios, reduce costos y facilita la convergencia. Con la facilidad que brinda IP es sencillo utilizar un servicio de datos para cursar llamadas de voz como datos para luego recuperarlas. Esta alternativa permite mejorar la competitividad de las empresas y reducir los precios en el mercado, sin embargo para aquellas empresas cuyo negocio es la telefonía puede acarrear efectos negativos.

2.4.3 COMPRA Y VENTA DE MINUNTOS EN INTERNET

En el mercado de las telecomunicaciones a nivel mundial se ha envuelto en el mundo del Internet. Con portales mucho más dinámicos y accesibles, posibilidades de pago más sencillas y eficientes, el Internet se ha convertido en

una plataforma ideal para la negociación de servicios, entre ellos los de telecomunicaciones.

Para el mercado de tráfico internacional, en Internet se han desarrollado portales WEB que reúnen a proveedores y usuarios. En estos portales se puede comprar y vender minutos de telefonía TDM, VoIP u otros servicios de telecomunicaciones. Algunas de las empresas más representativas del sector, como Arbinet, han desarrollado software o portales dedicados que permiten a sus usuarios interactuar con ofertas y demandas de diferentes partes del mundo facilitando el comercio.

Adicionalmente a los portales, en Internet es sencillo encontrar foros de discusión que se han convertido en pequeños mercados de telecomunicaciones. En estos foros los proveedores y usuarios, legales o no, ofrecen y demandan servicios de una manera más directa que la de los portales.

2.4.3.1 Arbinet

Arbinet es una compañía fundada en 1996, con el nombre de *Smart Group Holdings, Inc.*, y en el año 2009 cambia por última vez su nombre a Corporación Arbinet. Dedicada desde sus inicios a los servicios de telefonía, hoy en día ofrece Internet y conexión telefónica a más de 1300 destino en todo el mundo. Es considerado uno de los mercados para compra y venta de minutos más grande del mundo. [29]

Arbinet cuenta con un portal que permite a sus miembros interactuar con compradores y vendedores de servicios de telefonía alrededor del mundo y facilitar la compra y venta de tráfico. Arbinet se encuentra presente en Nueva York, Los Ángeles, Miami, Londres, Frankfurt y Hong Kong, y cuenta con equipos de venta en Norte América, América Latina, Europa, África y Asia, con lo cual mantiene cobertura global.

Arbinet ofrece distintos servicios de telefonía y voz entre los que destacan el de *carrier* internacional y el mercado de compra y venta de minutos, ambos para telefonía. Puntualmente los servicios que ofrece Arbinet son: [29]

- "*thexchange*".- Este servicio permite a los usuarios crear rutas de tráfico personalizadas sobre la plataforma que ofrece Arbinet. Posee el servicio RPG que crea automáticamente planes de direccionamiento cada 4 horas.
- *Servicios de carrier*.- Este servicio ofrece interconexión global utilizando como *carrier* la red de Arbinet. Las rutas se basan en las necesidades del usuario.
- "*Private Exchange*".- Permite crear una ruta de direccionamiento virtual y directa. Este servicio es dedicado y permite también la conversión de TDM a VoIP. Arbinet mantiene un control bilateral sobre la ruta y sus tasas de utilización.

Para inscribirse es necesario contactarse con un representante, especificar el tipo de servicio al que se desea inscribirse y cumplir con los aspectos técnicos y legales. Es importante mencionar que 18 de los 20 *carriers* más grandes en el mundo se encuentran conectados y utilizan a la red de Arbinet. [2]

En la Figura 2.16 se presenta la vista del portal desarrollado por Arbinet para la compra y venta de minutos. En este portal se puede observar que los términos de calidad para la red se establecen en función de su ASR y ACD.

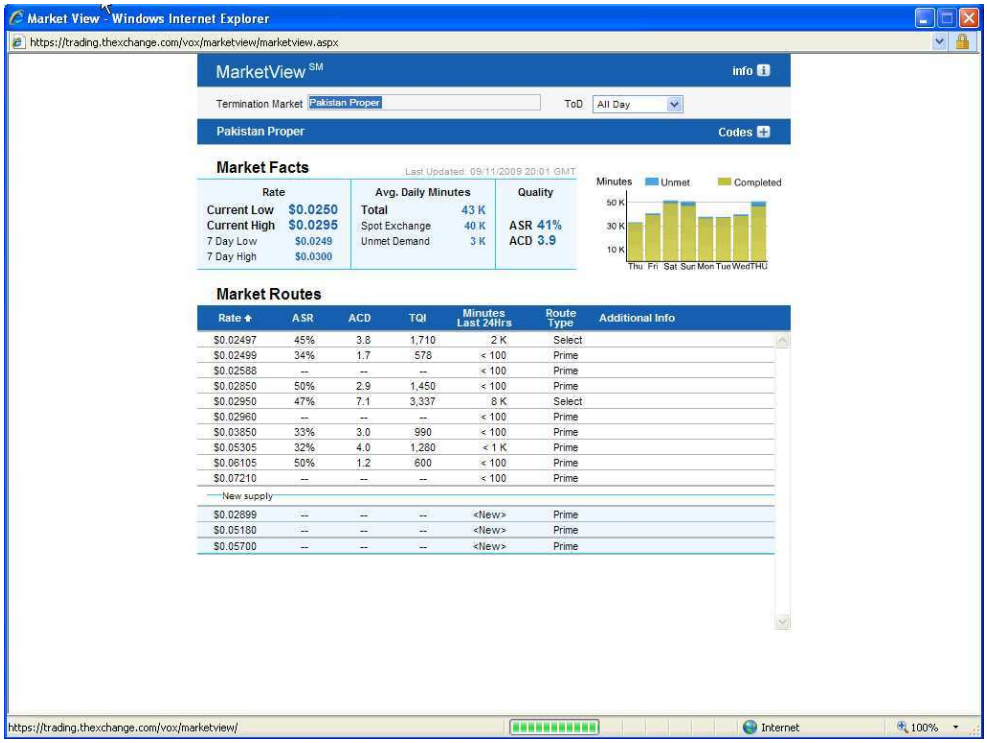


Figura 2.16. Vista del portal de negociación de Arbinet [29]

2.4.3.2 DirectInterconnect

Directinterconnect.com nace como la solución a una falta de sitios para encontrar y negociar rutas de tráfico telefónico. Directinterconect se establece como una red social que junta a proveedores y usuarios de servicios de VoIP. Esta red permita encontrar rutas y tarifas hacia varios destinos en el mundo a través de su foro. [33]

En otras palabras, este portal reúne a varias empresas de telecomunicaciones y permite encontrar una ruta directa hacia el país deseado a través de una compañía afiliada que ofrezca el servicio. Para esto se debe registrar en la página con lo cual se puede acceder a los datos de las compañías y sus requerimientos.

Una vez que se ha accedido al portal, se puede buscar una compañía que ofrezca el servicio que se desea comprar o viceversa para establecer contacto con un representante y proceder a negociar. Las compañías tienen propuestas tanto de compra como venta de minutos; y, en algunos casos exigen ciertos niveles de ASR y ACD. [33]

En la Figura 2.17 se puede observar el sistema de búsqueda que se utiliza. El tipo de protocolo que se utiliza depende de cada compañía. [33]

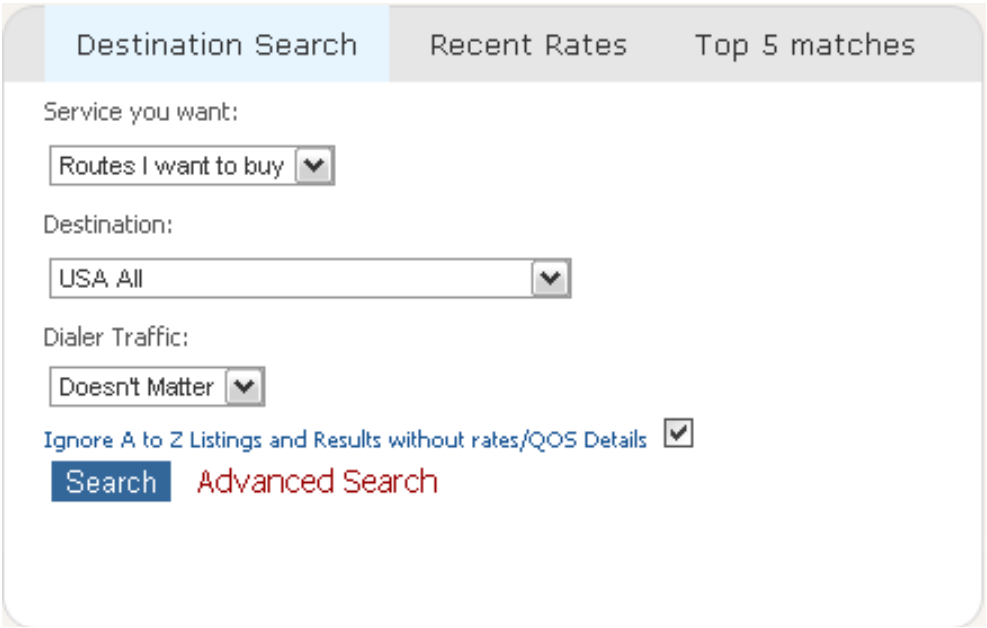


Figura 2.17. Búsqueda de compañías en directinterconect.com [33]

2.4.3.3 Tseyva Ltd. y EXCILA Telecom

EXCILA Telecom es una empresa de Singapur que ofrece servicios de telecomunicaciones a través de Tseyva Ltd. Tseyva Ltd. es una empresa que ofrece principalmente el servicio de reventa de minutos VoIP. EXCILA Telecom es subsidiaria de Tsayva Ltd. y ofrece al usuario un portal más sencillo de interacción. [36]

EXCILA Telecom es un *carrier* internacional que permite, a través de su portal web, comprar y vender tráfico telefónico. Trabaja utilizando VoIP y es sencillo acceder a sus servicios, para lo cual es necesario registrarse en la página web y realizar una oferta o demanda, según sea el caso. Trabaja utilizando códec G.729 o G.723. [36]

2.4.3.4 MinuteTraders

Un portal bastante importante para la compra o venta de minutos de telefonía es MinuteTraders. Este es un mercado virtual de telecomunicaciones donde tanto ofertantes como demandantes se presentan para negociar rutas y terminación en varios países. El esquema de funcionamiento del mercado es similar al de Arbinet. [48]

MinuteTraders tiene una característica particular, y es que dada la demanda de rutas el acceso a este mercado está restringido y solo se puede hacer a través de una invitación. Su política es mantener un control sobre la cantidad de participantes por lo que para registrarse primero se debe registrar una cuenta de correo a través de la cual, según dispongan, se envía una invitación. Una vez registrado en el portal, se accede o se crea a una sala de negociación donde se presentan ofertas de terminación. El interesado debe escoger una ruta sea para vender o comprar minutos, y según el caso presentar o recibir ofertas de *carriers* interesados. Dependiendo de cómo se concrete la negociación se establece la conexión con el *carrier*. [48]

El portal que ofrece MinuteTraders es sencillo de utilizar y permite escoger entre destinos y rutas que se deseen negociar con varios países. Adicionalmente se presenta información sobre la calidad de las redes, disponibilidad, etc.

2.4.3.5 IPsmarx

IPsmarx es una compañía que ofrece soluciones de VoIP a nivel internacional desde el 2001. Con presencia en alrededor de 60 países, esta empresa ofrece terminación de telefonía con VoIP en cualquier parte del mundo utilizando protocolos SIP y H.323 para la conexión. [43]

IPsmarx no provee un mercado de compra y venta de minutos entre proveedores. Es una compañía que provee servicios entre los cuales vende minutos de terminación internacional actuando como *carrier*. Sin embargo, podemos considerarla como un portal ya que también recibe ofertas para la compra de minutos. [43]

Para negociar la compra o vente de una ruta primero se debe incluir una propuesta acorde con el formulario que se presenta en la página web de la empresa en la sección de terminación internacional. [43]

2.4.3.6 2GoTEL

2GoTel es básicamente un *carrier* de telefonía que ofrece tanto terminación como compra de minutos. No se trata de un portal propiamente, sin embargo un proveedor del servicio puede comprar o vender sus rutas a 2GoTEL a través de su página web, y tan solo presentando una oferta o requerimiento. [27]

2GoTEL ofrece terminación en cualquier destino del mundo además de otros servicios de telefonía. Para ofrecer o comprar una ruta de tráfico es necesario llenar los formularios que se encuentran en su página WEB con los datos de la ruta deseada. Este formulario es enviado y la compañía decide como negociar el servicio. [43]

2GoTEL es una compañía del sector de telecomunicaciones que trabaja con VoIP y que, a diferencia de Arbinet o MinuteTrades, no provee un portal de negociación para diferentes proveedores y clientes. [43]

2.4.3.7 TerraSIP

Otro portal que permite negociar VoIP es TerraSIP. Esta compañía brinda servicios de comunicaciones con VoIP que de la misma forma que VoIP.ms o

2GoTel ofrece una variedad de servicios que incluyen DID's internacionales, terminación de telefonía y SMS. [60]

Para este estudio el servicio de *carrier-to-carrier* es el más relevante. Como *carrier* de telefonía permite comprar minutos. También ofrece la posibilidad de vender minutos a través de un correo a una dirección WEB. La oferta debe ser presentada para que la compañía decida si aceptarla o no. [60]

Es importante mencionar que TerraSIP soporta protocolo SIP principalmente, y utiliza G711 / G729 / G723 / G726 / iLBC / GSM como códecs de telefonía. [60]

2.4.3.8 VoIP.ms

Entrando en las compañías que venden o revenden tráfico de VoIP está VoIP.ms, una empresa norteamericana que adicionalmente ofrece minutos hacia cualquier parte del mundo. Entre los servicios que ofrece están DID's internacionales, terminación y reventa. [72]

Si bien esta página puede ser utilizada para realizar pruebas SISLAC, no compra minutos de telefonía a través de su portal lo cual sugiere que conoce el tipo de rutas que utiliza para enviar o recibir tráfico telefónico. [72]

2.4.3.9 Foros de compra y venta de minutos

Los portales para negociación de tráfico son una alternativa para comprar o vender minutos, sin embargo en Internet ha surgido un método alternativo mediante la utilización de foros. Los foros de discusión facilitan a una persona opinar o comentar un tema en particular, en este caso ofrecer un punto de terminación en un determinado país o demandar minutos.

A diferencia de los portales, en un foro de negociación no existe un intermediario directo que ofrezca el encuentro, tan solo los interesados en comprar o vender tráfico que negocian. Ya que no existe una plataforma común, a través de mensajes privados las partes se ponen de acuerdo para su transacción y la conexión se realiza de forma directa.

Es importante diferenciar las rutas que se pueden encontrar en un foro de negociación. No todas las rutas son legalmente autorizadas en un país u otro por

lo cual se les ha dado comúnmente una clasificación de blanca, gris o negra. Como ejemplo figurativo, supongamos se origina una llamada con origen en España y destino en Ecuador: [61]

- Ruta blanca (*white route*).- Se conoce como ruta blanca a aquella ruta que es legal tanto en el país de origen como en el país de destino. En este ejemplo, se utilizan rutas reconocidas como legales tanto en España como en Ecuador.
- Ruta gris (*gray route*).- Se denomina como ruta gris a aquellas rutas que son legales en el país de origen, sin embargo no lo son en el país de destino. Es decir, son legalmente originadas en España, sin embargo la ruta no es considerada legal en Ecuador.
- Ruta negra (*black route*).- Como su nombre lo supone, se refiere a aquellas rutas que no son legales en el país de origen aunque pueden serlo en el país de destino. Una llamada se origina por una ruta ilegal en España, aunque la ruta en Ecuador se considere legal.

Los sistemas “bypass” se los clasificaría entonces como de rutas grises o negras. En detalle una ruta gris no es necesariamente una ruta considerada como “ilegal” sino que se entiende que en algún punto de la ruta alguna compañía está perdiendo dinero. En este concepto se puede incluir el REFFILING, donde se utilice una operadora intermediaria para reducir el costo de interconexión. Aunque ambas rutas pueden ser legales, entre los países de origen y destino con la operadora, la ruta no es la esperada y representa un perjuicio.

Estos términos son comúnmente utilizados en los foros de negociación de tráfico, en especial rutas blancas y grises, ya que las rutas grises se caracterizan por ofrecer un costo menor al de una ruta blanca, a expensas de no garantizar calidad en la comunicación. Las rutas grises surgieron para hacer que las llamadas internacionales sean más baratas, es decir como una alternativa pensada para abaratar costos y para usuarios que no consideran importante la calidad.

En un foro de negociación, es común encontrar clasificadas sus salas en rutas blancas y rutas grises. Las rutas negras, por lo general, no son consideradas en estos foros. En cuanto al delito del “bypass”, las rutas grises son una forma

sencilla y práctica para un defraudador de presentarse en el mercado y ofrecer minutos de telefonía. Además brinda la seguridad del anonimato que ofrece un foro en internet por lo que no implica un riesgo directo.

2.5 EL ECUADOR Y LOS DELITOS EN TELECOMUNICACIONES [12]

Los esfuerzos que la Fiscalía y SUPERTEL realizan en el combate a los sistemas telefónicos “bypass” están amparados en las disposiciones legales vigentes en el Ecuador. El Ecuador cuenta con una Ley Especial de Telecomunicaciones, publicada en el Registro Oficial No. 996 del 10 de agosto de 1992 y sus reformas, que regulan la instalación y operación de servicios de telecomunicaciones.

En cuanto al aspecto penal, los delitos en telecomunicaciones son considerados en el artículo 422 del código penal, reformado mediante la “Ley Reformatoria al Código Penal No. 99-38” publicada en el Registro Oficial No. 253 del 12 de agosto de 1999. El artículo textualmente cita:

> “*Art. 422.- Será reprimido con prisión de seis meses a dos años el que interrumpiere la comunicación postal, telegráfica, telefónica, radiofónica o de otro sistema, o resistiere violentamente al restablecimiento de la comunicación interrumpida.*
>
> *Si el acto se realizare en reunión o en pandilla, o la interrupción fuere por medios violentos, vías de hecho o amenazas, la pena será de prisión de tres a cinco años.*
>
> *Quienes ofrezcan, presten o comercialicen servicios de telecomunicaciones, sin estar legalmente facultados, mediante concesión, autorización, licencia, permiso, convenios o cualquier otra forma de la contratación administrativa, salvo la utilización de servicios de internet, serán reprimidos con prisión de dos a cinco años.*
>
> *Estarán comprendidos en esta disposición, quienes se encuentren en posesión clandestina de instalaciones que, por su configuración y demás datos técnicos, hagan presumir que entre sus finalidades está la de*

destinarlos a ofrecer los servicios señalados en el inciso anterior, aun cuando no estén siendo utilizados.

Las sanciones indicadas en este artículo, se aplicarán sin perjuicio de las responsabilidades administrativas y civiles previstas en la Ley Especial de Telecomunicaciones y sus Reglamentos". [12]

Para llevar a cabo el proceso de juzgamiento en muchos casos de este tipo de fraudes, es necesario incluir en el estudio del caso otras figuras legales contenidas en diferentes leyes, como la Ley de Defensa al Consumidor, a fin de tener los elementos suficientes para sancionar a un defraudador. En las circunstancias actuales y con el avance de la tecnología, sin duda es necesaria una actualización en nuestras leyes y en el código penal que estipule y sancione cada delito de redes y telecomunicaciones de forma particular, y permita a la SUPERTEL ejercer un mayor control sobre este tipo de delitos.

CAPÍTULO 3

DESARROLLO E IMPLEMENTACIÓN DEL SISTEMA

3.1 REQUISITOS Y NECESIDADES DE LA SUPERINTENDENCIA [32]

Como se ha analizado, los sistemas telefónicos “bypass” son en la actualidad uno de los fraudes más comunes y con mayor impacto. Por este motivo y acorde con sus funciones de control, la Superintendencia de Telecomunicaciones trabaja sin descanso en busca de soluciones tecnológicas que contribuyan al combate de este tipo de delito.

3.1.1 REQUERIMIENTOS DE LA SUPERINTENDENCIA

La Superintendencia de Telecomunicaciones cuenta con un programa para realizar pruebas de lazo cerrado de forma automática que utiliza dos teléfonos celulares. Sin embargo, dicho software presenta varias limitaciones en cuanto a

las llamadas simultáneas, que hacen a la SUPERTEL requerir una solución más versátil y amplia. En base a las necesidades recogidas de la Dirección Nacional de Investigación Especial en Telecomunicaciones, se pudo determinar que la SUPERTEL requiere un sistema que cumpla al menos con las siguientes funciones:

- Realizar y recibir llamadas de prueba de lazo cerrado utilizando tarjetas de telefonía pre-pagada, y generar CDR's.
- Realizar y recibir varias llamadas de prueba de forma simultánea utilizando líneas de telefonía fija y/o telefonía celular, y generar CDR's.
- Programar la ejecución de pruebas de lazo cerrado utilizando tarjetas de telefonía pre-pagada.
- Identificar el número identificador de llamada (*Caller ID*) de las llamadas recibidas y evaluar si pertenece a un origen nacional o internacional.
- Emitir una notificación vía e-mail al momento de recibir un número nacional en una prueba de lazo cerrado.
- Manejar una base de datos de tarjetas de telefonía pre-pagada disponibles.
- Mantener un registro de las llamadas de prueba realizadas.
- Guardar los datos de la base de datos en PDF u hojas de cálculo.
- Mostrar estadísticas sobre las tarjetas utilizadas.
- Cambiar los números telefónicos utilizados para generar y recibir las llamadas con facilidad, según sea necesario.
- Configurar los aspectos importantes del programa de forma sencilla.

Para determinar si una llamada entrante se la considera sospechosa, se debe identificar el tipo de número origen que posee, evaluando el número de identificador de llamante (*Caller ID*). El número será evaluado en base a las siguientes consideraciones para determinar si es un número sospechoso: [32]

1. Que esté formado por 9 dígitos.
2. Que corresponda a un número de telefonía fija nacional, es decir, que inicie con los prefijos e indicativos utilizados en Ecuador para telefonía fija (02, 03, 04, 05, 06, 07).
3. Que corresponda a un número de telefonía móvil nacional, es decir, que inicie con los prefijos e indicativos utilizados en Ecuador para telefonía móvil (06, 08, 09).

Finalmente, de las pruebas de lazo cerrado realizadas utilizando el sistema se debe registrar al menos la siguiente información:

- Fecha y hora de la llamada recibida.
- Número de identificación de llamada recibida (*Caller ID*).
- Duración de la llamada.
- Número de origen y destino.
- Tarjeta utilizada.

3.1.2 PLANTEAMIENTO DE LA SOLUCIÓN

Para establecer la solución más adecuada es conveniente considerar diferentes alternativas, identificando sus pros y contras. De los requerimientos listados, cabe destacar que los aspectos más trascendentales para esta solución radican en la generación y recepción de llamadas, así como en la identificación del número llamante.

Además, la solución a implementarse debe manejar la información de las tarjetas disponibles para que sean utilizadas en las llamadas de prueba. También debe registrar los datos de las llamadas realizadas y recibidas. Esta información debe ser contenida en bases de datos a fin de que pueda ser utilizada para generar documentos con información sobre las pruebas ejecutadas y los resultados obtenidos.

La función de generar reportes facilita de gran manera el trabajo de consolidar la información de pruebas y resultados. Con esta información se puede proceder a realizar una investigación de los números telefónicos detectados. Adicionalmente, la información almacenada en la base de datos constituye un respaldo digital.

Figura 3.1. Diagrama general de los componentes del sistema

En la Figura 3.1 se observa un diagrama de los principales servicios del sistema que se lo denominará ASTEM. Como función principal, el sistema debe contar con un gestor de llamadas flexible que permita realizar y recibir llamadas simultáneas, además de cambiar los números utilizados con facilidad. Considerando este primer problema, se cuenta con tres alternativas:

1. Utilizar un grupo de módems telefónicos.
2. Utilizar una PBX ASTERISK.
3. Utilizar una PBX ELASTIX.

La identificación y análisis del *Caller ID*, así como el envío de notificaciones, son aspectos importantes para tener en cuenta durante el desarrollo ya que permiten automatizar el procedimiento de notificación cuando se detecta una línea

involucrada a un posible “bypass”. Ésta es una funcionalidad que permite a los usuarios conocer los números sospechosos en el momento en que una llamada ingresa al sistema, lo cual facilita tomar acciones inmediatas agilizando los procesos de combate a este tipo de fraude.

3.1.2.1 Análisis de una solución utilizando un grupo de módems telefónicos

En primer lugar, utilizando módems adecuados es posible originar y recibir llamadas programando su duración. El desarrollo e implementación del software debe concentrarse en la comunicación con los módems que se vayan a utilizar, debido a que este debe controlar únicamente las instrucciones para que estos módems generen y reciban las llamadas.

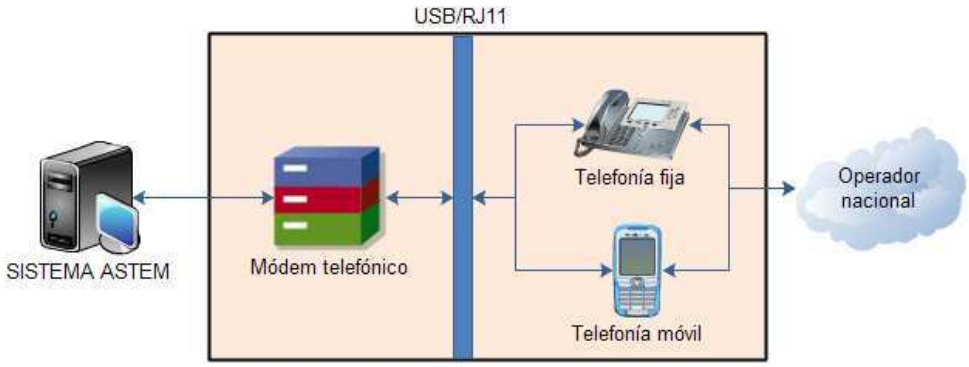


Figura 3.2. Gestor de llamadas utilizando módems

Por otro lado, se debe destacar que esta solución requiere utilizar equipos compatibles entre sí; es decir, para realizar llamadas utilizando líneas de telefonía móvil, es necesario contar con equipos celulares compatibles con el hardware del computador y que puedan ser controlados por el software que gestiona las llamadas. De igual forma sucede con las líneas de telefonía fija y los módems que sean necesarios para éstas.

La compatibilidad del hardware presenta un inconveniente muy grande ya que dificulta cambiar de equipos o realizar actualizaciones. Este inconveniente también afecta al software, ya que este tendrá que ser desarrollado para manejar específicamente los módems previstos para la solución. Como se diagrama en la Figura 3.2, el módem telefónico se conecta directamente con el computador (puerto PCI), y con la línea telefónica a través de un cable USB o RJ11. Por cada módem usualmente se conecta 1 línea telefónica.

El manejo de llamadas simultáneas presenta un problema adicional y bastante complejo ya que por cada llamada de lazo cerrado se necesitará un computador y un par de módems. Tanto en telefonía móvil como fija, la cantidad de módems que se pueden conectar al computador es baja por la cantidad de puertos disponibles.

3.1.2.2 Análisis de una solución utilizando una PBX ASTERISK o ELASTIX

La utilización de una PBX ASTERISK o una PBX ELASTIX facilita la gestión de llamadas y permite tener un registro de CDR's local en la PBX propio de ASTERISK. Estas PBX pueden trabajar con tarjetas de telefonía analógica, en cuyo caso permite conectar y desconectar líneas de telefonía fija o móvil de forma sencilla. En el caso de líneas de telefonía móvil es necesario utilizar una base celular por cada línea.

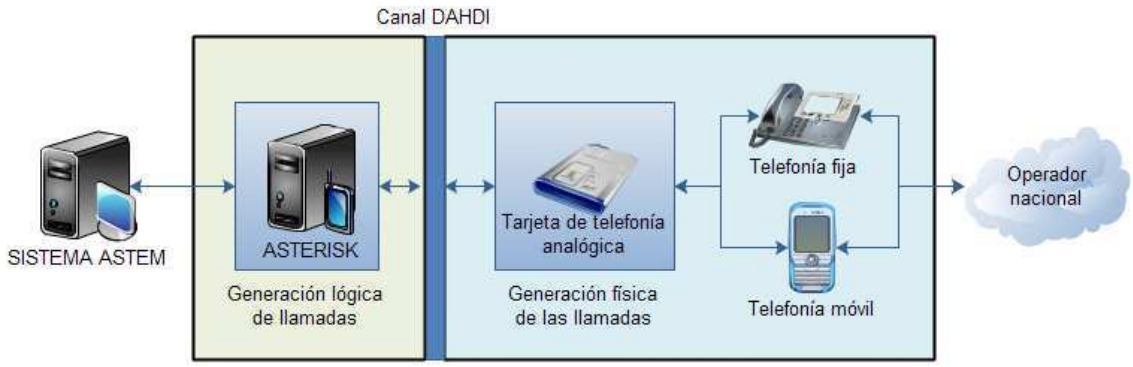


Figura 3.3. Gestor de llamadas utilizando ASTERISK

Una de las principales ventajas de utilizar una PBX es que permite diferenciar en dos fases el proceso de cada llamada. La primera fase se encarga de la generación y recepción final de las llamadas, es decir, indica el marcado de las llamadas salientes y recibe las llamadas entrantes. Esta etapa sería controlada por la PBX, como se observa en la sección “Generación lógica de llamadas” de la Figura 3.3.

La segunda fase, correspondiente a la sección “Generación física de las llamadas” en la Figura 3.3, es la encargada de conectar las llamadas con una línea telefónica según el tipo de línea que se utilice. Por ejemplo, una llamada de telefonía móvil utilizará una base celular, mientras que una llamada de telefonía fija una línea telefónica convencional.

Esta diferenciación permite al sistema utilizar el mismo motor de llamadas, es decir la PBX ASTERISK o ELASTIX, sin diferenciar si las líneas conectadas son de telefonía fija o móvil. Se pueden conectar varias líneas a la PBX utilizando una sola tarjeta de telefonía analógica.

Por otro lado, la implementación de esta solución presenta un reto en cuanto al software. Es necesario considerar que para varias llamadas, el software debe colocar en la PBX el número correcto de llamadas cada cierto tiempo y verificar que no más de una llamada utilice una misma línea, a fin de que todas las llamadas se ejecuten en su totalidad y sin que sean bloqueadas por la falta de líneas disponibles.

La PBX ASTERISK y PBX ELASTIX reúnen funcionalidades muy similares, sobre todo considerando que la PBX ELASTIX es un software desarrollado sobre ASTERISK que implementa una interfaz gráfica para facilitar su configuración; sin embargo, la interfaz gráfica de ELASTIX puede representar una limitación para los fines de este trabajo, ya que las configuraciones que se necesitan en el sistema difieren mucho las configuraciones de una central telefónica tradicional. En el mismo sentido, muchos de los servicios configurados por defecto en ELASTIX no contribuyen a esta aplicación en particular, sino que incluso pueden resultar contraproducentes ya que la configuración de estos sistemas es conocida por muchas personas lo cual implica riesgos de seguridad.

3.1.2.3 Solución con módems vs PBX ASTERISK vs ELASTIX

Con base en los análisis realizados de las diferentes alternativas para el gestor de llamadas, se evalúa a cada una en base a un listado de criterios. Estos criterios han sido recogidos de las necesidades de la SUPERTEL y discutidos con funcionarios de la Dirección Nacional de Investigación Especial en Telecomunicaciones.

Cada criterio es calificado en las tres alternativas con una nota entre 1 y 10, donde 1 representa la peor calificación, y 10 la mejor. En la Tabla 3.1 se puede observar los criterios definidos para este análisis y la evaluación correspondiente a cada alternativa.

Criterio	Solución Módems	PBX ASTERISK	PBX ELASTIX
Menor cantidad de equipos	4	8	8
Escalabilidad del sistema	6	8	7
Facilidad de configuración del sistema	5	9	7
Facilidad de configuración de las tarjetas	4	10	10
Interfaz gráfica del sistema	10	10	10
Compatible con VoIP	4	10	10
Facilidad en el aumento de líneas	4	10	10
Manejo simultáneo de telefonía fija y móvil	5	10	10

Tabla 3.1. Matriz de valoración de alternativas para el gestor de llamadas

En base a los valores definidos en la Tabla 3.1 para cada alternativa del gestor de llamadas, se procede a su evaluación en función del peso que cada criterio tiene para la SUPERTEL. Los pesos detallados en la Tabla 3.2 han sido definidos en coordinación con la Dirección Nacional de Investigación Especial en Telecomunicaciones de la SUPERTEL.

Cada criterio representa, en su peso, un porcentaje del total. Es necesario aclarar que las soluciones con PBX ASTERISK y PBX ELASTIX son muy similares en cuanto a funcionalidades; sin embargo, ASTERISK ofrece mayor libertad de configuración ya que trabaja directamente con el código de la PBX. Por su parte, ELASTIX es un sistema basado en ASTERISK que viene configurado para cumplir funciones tradicionales de una central telefónica y su interfaz gráfica no ofrece la misma libertad de configuración que ASTERISK.

Como se mencionó anteriormente, el sistema a implementarse requiere adaptar las funcionalidades de la PBX a las necesidades de la SUPERTEL, por lo que la configuración y los servicios que incluye ELASTIX resultan contraproducentes. Por este motivo y en este caso en particular, se ha dado una menor valoración a ELASTIX en “Escalabilidad del sistema” y “Facilidad de configuración del sistema” respecto a ASTERISK.

Criterio	Peso	Módem telefónico		PBX ASTERISK		PBX ELASTIX	
		Val	Pon	Val	Pon	Val	Pon
Menor cantidad de equipos	0,1	4	0,4	8	0,8	8	0,8
Escalabilidad del sistema	0,2	6	1,2	8	1,6	7	1,4
Facilidad de configuración del sistema	0,1	5	0,5	9	0,9	7	0,7
Facilidad de configuración de las tarjetas	0,1	4	0,4	10	1	10	1
Interfaz gráfica del sistema	0,1	10	1	10	1	10	1
Compatible con VoIP	0,1	4	0,4	10	1	10	1
Facilidad en el aumento de líneas	0,15	4	0,6	10	1,5	10	1,5
Manejo simultáneo de telefonía fija y móvil	0,15	5	0,75	10	1,5	10	1,5
TOTAL	**1**	**-**	**5,25**	**-**	**9,3**	**-**	**8,9**

Tabla 3.2. Matriz de decisión de alternativas para el gestor de llamadas

Como se puede observar, la evaluación de cada alternativa con su valor ponderado correspondiente muestra que el sistema implementado con PBX ASTERISK es la mejor alternativa. En adición, a la SUPERTEL le interesa trabajar con una solución de este tipo ya que ofrece mayores aplicaciones futuras por su completa compatibilidad con protocolos VoIP.

3.1.2.4 Sistema gestor de llamadas ASTEM

En base al análisis realizado en el apartado 3.1.2.3 de este trabajo, se opta por el desarrollo del sistema gestor de llamadas utilizando una PBX ASTERISK.

Para almacenar los registros más relevantes de ASTERISK y del sistema, se utiliza el motor de base de datos MySQL. Este motor de base de datos es software libre y trabaja perfectamente con ASTERISK sobre entornos LINUX. Los

demás datos y configuraciones del programa podrán ser almacenados en archivos de configuración.

En cuanto a la notificación de alertas, se utiliza un servidor de correo electrónico local y otro externo de respaldo. Una vez que el software identifique entre las llamadas entrantes un número que cumpla con los parámetros de evaluación, se conecta a un servidor de correo electrónico para enviar un e-mail con los datos más relevantes de dicha llamada.

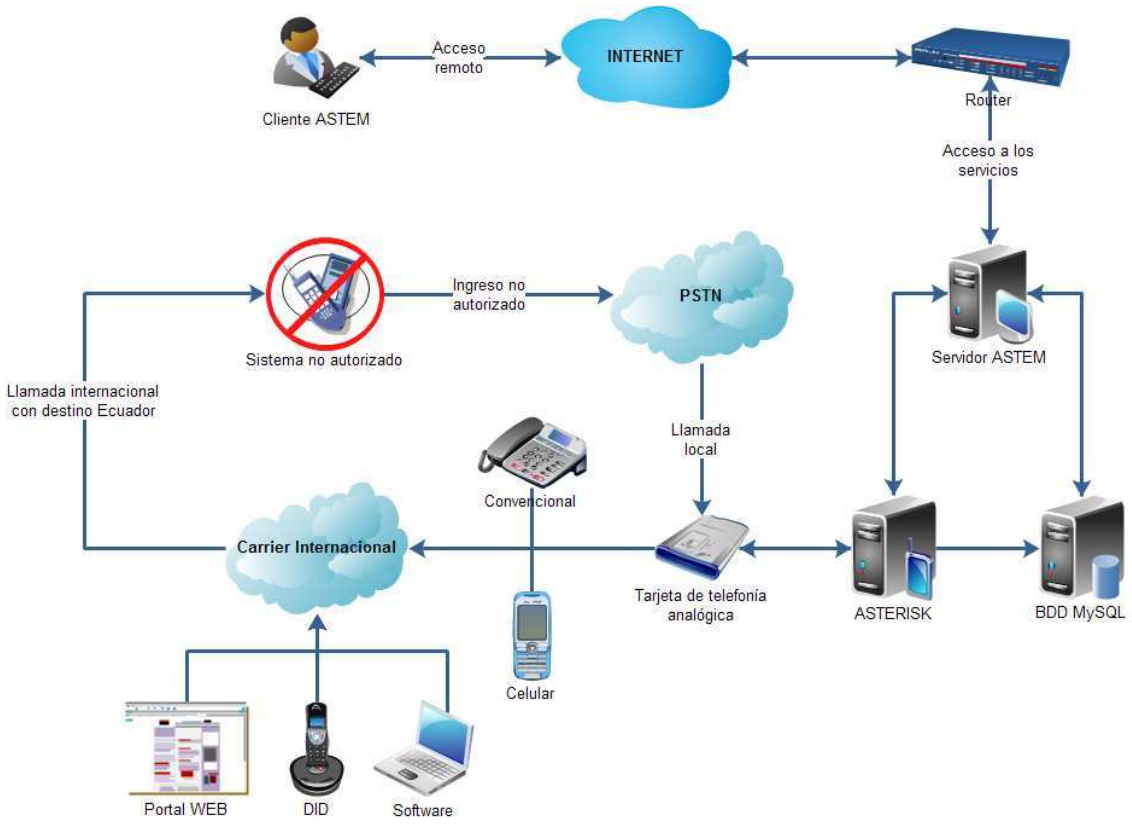


Figura 3.4. Diagrama del sistema gestor de llamadas ASTEM

Los usuarios del sistema serán funcionarios de la SUPERTEL familiarizados principalmente con el sistema operativo Windows. Por esto, para su facilidad, el software será diseñado como una aplicación distribuida tipo cliente-servidor, como se observa en la Figura 3.4. Esto permite acceder al sistema a través de una aplicación de escritorio en Windows, desde la cual será posible controlar el funcionamiento del sistema y su configuración.

En adelante, al software desarrollado en esta solución se lo denominará ASTEM.

3.1.3 SELECCIÓN DEL SOFTWARE

Como se analizó en el Capítulo 1, los lenguajes de programación considerados como alternativas para el sistema ASTEM comparten muchas similitudes. En la Tabla 3.3 se observa una comparación de algunos aspectos de los lenguajes, a fin de evaluarlos de una manera más objetiva.

Característica	C#	JAVA	PHP
Licencia libre		x	x
Programación orientada a objetos	x	x	x
Manejo de hilos	x	x	
Multiplataforma		x	x
Escalabilidad	x	x	x
Integración con bases de datos MySQL	x	x	x
Integración con servicios de ASTERISK	x	x	
Seguridad	x	x	x

Tabla 3.3. Comparación de los lenguajes de programación

Para el desarrollo del sistema ASTEM que controlará la actividad de la central se utiliza el lenguaje de programación JAVA por dar mayor facilidad en el manejo de hilos, ser software libre, ser independiente de la plataforma donde se ejecute y permitir la conexión con otros programas desarrollados en distintos lenguajes. Se opta por aprovechar el manejo multitarea más allá de las ventajas que ofrece PHP en cuanto al entorno gráfico, lo cual puede ser compensado con una aplicación cliente de escritorio amigable.

3.1.4 DIMENSIONAMIENTO DE LOS ELEMENTOS

Normalmente al hablar de una central telefónica se debe considerar en su diseño el tráfico que va a cursar, concurrencia de los usuarios, tiempo promedio por

llamada, grado de disponibilidad del servicio, etc. Como se detalló en la sección 1.3, comúnmente se calcula la cantidad de líneas en una central telefónica utilizando los modelos estadísticos de Erlang B y C. Sin embargo, para este trabajo las consideraciones de dimensionamiento de la PBX deben ser diferentes ya que las funciones de la central telefónica no son las convencionales.

Una central telefónica, en la mayoría de casos, está orientada a procesar llamadas de usuarios, entre ellos y hacia la red pública. En este trabajo, la central telefónica no procesará ninguna llamada desde una extensión, y en adición, no se tendrá usuarios configurados en el sistema. La PBX será utilizada para procesar llamadas automáticas originadas en el sistema ASTEM, las cuales no requieren de una extensión que las inicie. Además, el sistema necesita dos líneas disponibles para cada llamada de lazo cerrado, por lo que es necesario garantizar dicha cantidad de líneas.

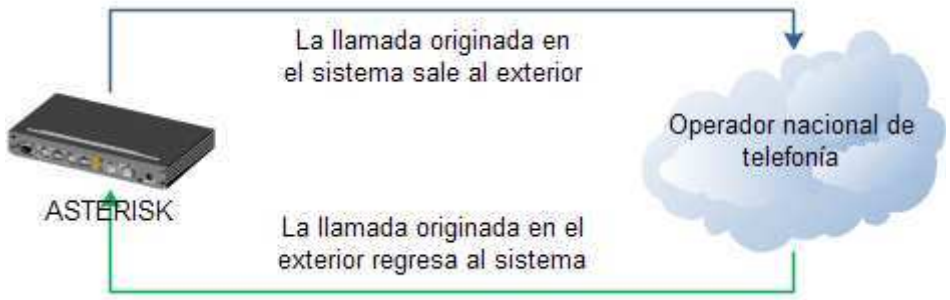


Figura 3.5. Diagrama de las dos etapas en una llamada de lazo cerrado

La PBX debe realizar y recibir las mismas llamadas en líneas distintas, es decir, debe utilizar una línea telefónica para iniciar una llamada y una diferente para recibirla, como se observa en el diagrama de la Figura 3.5. Es un requisito que ambas líneas telefónicas estén disponibles, por lo cual no hace falta determinar grados de disponibilidad, ya que en este caso sería 1.

Por otro lado, tampoco hace falta definir un tiempo promedio de las llamadas (ACHT) ya que cada llamada de lazo cerrado tendrá una duración máxima durante la cual las líneas telefónicas no deberán ser utilizadas. Este tiempo debe ser definido en el sistema ASTEM y configurado en la central ASTERISK para que ninguna llamada exceda este tiempo.

El dimensionamiento de esta PBX depende del número de llamadas de prueba que se deseen realizar simultáneamente. Por cada llamada de prueba de lazo cerrado es necesario conectar dos líneas telefónicas.

En este punto, es importante definir las características técnicas que debe tener el servidor ASTERISK para que le permita el aumento de líneas sin comprometer el rendimiento del sistema. No existe un método definido para dimensionar el hardware de un servidor de telefonía, sin embargo, varios foros en Internet recogen la experiencia de muchos usuarios con servidores ASTERISK de diferentes características.

Para corroborar la información disponible en Internet sobre servidores ASTERISK, se realizó una prueba donde se utilizó un servidor ASTERISK para realizar 2 llamadas simultáneas y verificar el impacto de estas llamadas en la utilización de recursos del computador.

En los resultados se pudo observar que cada llamada utiliza alrededor del 7 % de recursos del CPU, es decir, un equivalente a 128 MHz aproximadamente. Esto concuerda con información disponible en Internet donde se presentan las cifras descritas en la Tabla 3.4.

Propósito	Número de canales	Mínimo recomendado
Demostración	1 a 5	400 MHz x86, 256 MB RAM
Pequeña oficina/Hogar	6 a 10	1 GHz x86, 512 MB RAM
Pequeño negocio	11 a 25	3 GHz x86, 1 GB RAM
Mediana escala	Más de 25	Procesadores doble núcleo

Tabla 3.4. Recomendación de dimensionamiento de PBX ASTERISK [73] [64]

Estas especificaciones dependerán también del códec que se utilice en la PBX, sin embargo en la Tabla 3.4 se recoge información muy útil para dimensionar un servidor ASTERISK en la mayoría de casos.

En este trabajo se utilizará un computador Pentium IV de 1.8 GHz con 756 MB de memoria RAM y una tarjeta de telefonía analógica marca OpenVox A400P de 4 puertos FXO. Este equipo cumple con los requisitos mínimos recomendados para manejar simultáneamente las cuatro líneas de la tarjeta de telefonía.

3.2 DISEÑO DEL SISTEMA ASTEM

Una vez identificadas las principales funcionalidades que debe ofrecer la solución se puede estructurar los componentes del software que utilizará la PBX ASTERISK para generar y recibir llamadas de lazo cerrado.

Entre las técnicas de diseño descritas en la sección 1.6, UML destaca por ser un método orientado a objetos y ofrecer métodos que facilitan el modelado de sistemas en base a los requerimientos del usuario. La técnica de CASOS DE USO utilizada en UML permite distinguir las funciones que debe cumplir el sistema de manera sencilla y práctica. Por estos motivos, para efectos de este trabajo se utiliza UML como técnica de diseño, y se aplican los diagramas de CASOS DE USO y ACTIVIDAD.

3.2.1 CASOS DE USO

Una vez analizados los requerimientos de la SUPERTEL, se han defino los siguientes casos de uso para el sistema, representados en la Figura 3.6:

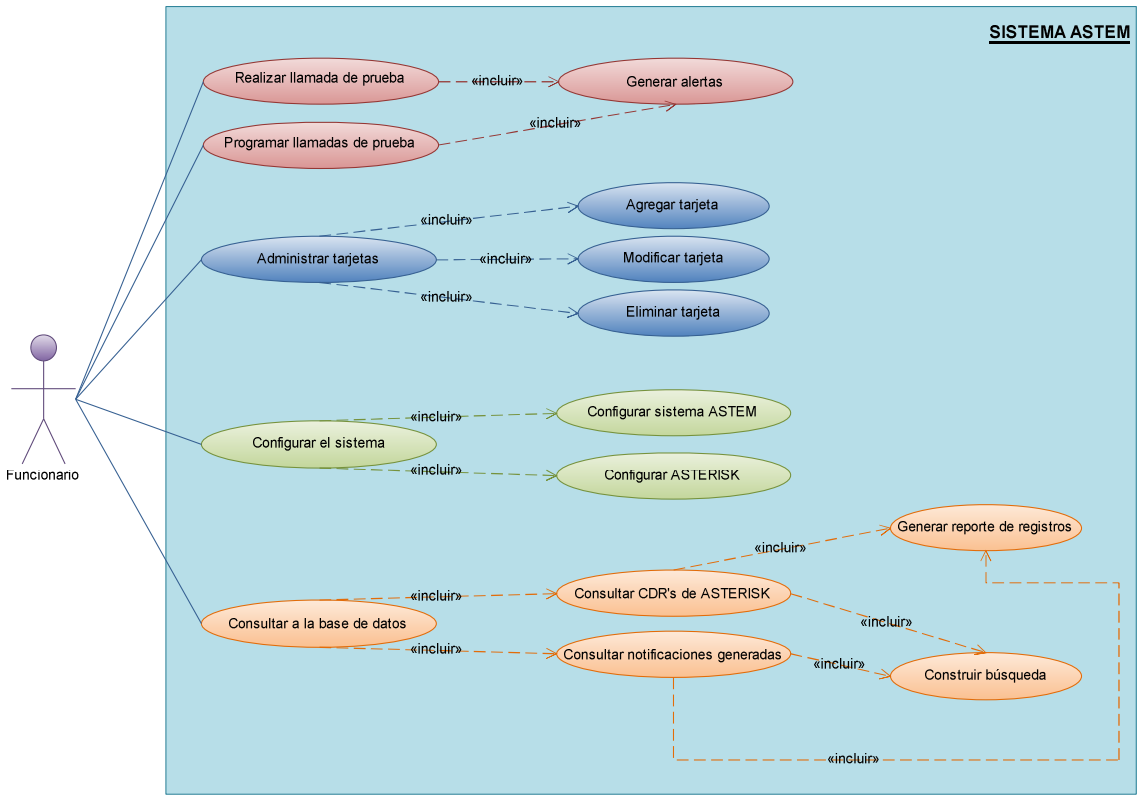


Figura 3.6. Diagrama de casos de uso del sistema

3.2.1.1 Acceder al sistema

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador debe decidir utilizar el programa para realizar pruebas de lazo cerrado.
Caso de éxito	1. Ingresa a la aplicación cliente. 2. Ingresa un usuario y contraseña. 3. Accede al sistema.
Caso alternativo	1. Ingresa a la aplicación cliente. 2. Ingresa un usuario y/o contraseña errónea. 3. Muestra mensaje de error. 4. Vuelve al paso 1.
Pos condiciones	- El administrador tiene acceso a las funcionalidades del sistema.

Tabla 3.5. Caso de uso "Acceder al sistema"

3.2.1.2 Salir del sistema

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador termina las tareas pendientes y se decide a cerrar el programa.
Caso de éxito	1. Desconecta el sistema de la aplicación servidor. 2. Cierra la ventana del sistema.
Caso alternativo	1. Cierra la aplicación cliente sin previa desconexión.
Pos condiciones	- Finaliza la aplicación.

Tabla 3.6. Caso de uso "Salir del sistema"

3.2.1.3 Realizar llamada de prueba

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos. - El administrador planea realizar una o más pruebas de lazo cerrado utilizando un par de líneas telefónicas y una sola tarjeta de telefonía pre-pagada.
Caso de éxito	1. Ingresa al generador de llamadas. 2. Selecciona la tarjeta que desea utilizar. 3. Selecciona el teléfono destino al que se realizarán las llamadas.

Característica	Descripción
	4. Seleccionar el teléfono de origen desde donde se realizarán las llamadas. 5. Define el número de llamadas que se realizarán. 6. Indica la generación de las llamadas.
Pos condiciones	- El programa regresa al menú principal.

Tabla 3.7. Caso de uso "Realizar llamada de prueba"

3.2.1.4 Programar llamadas de prueba

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos. - El administrador planea realizar varias pruebas de lazo cerrado utilizando un grupo de teléfonos y tarjetas de telefonía pre-pagada.
Caso de éxito	*Caso 1* 1. Selecciona el generador de llamadas. 2. Selecciona las tarjetas que desea utilizar. 3. Selecciona los teléfonos desde donde se originarán las llamadas. 4. Selecciona los teléfonos que recibirán las llamadas de prueba y la cantidad de llamadas a cada teléfono. 5. Define una fecha y hora para el inicio de las pruebas. 6. Se programan las pruebas en la aplicación servidor. *Caso 2* 1. Selecciona el generador de llamadas. 2. Selecciona las tarjetas que desea utilizar. 3. Selecciona los teléfonos desde donde se originarán las llamadas. 4. Selecciona los teléfonos que recibirán las llamadas de prueba y la cantidad de llamadas a cada teléfono. 5. Las pruebas en la aplicación servidor se ejecutan inmediatamente.
Pos condiciones	- La aplicación cliente regresa al menú principal.

Tabla 3.8. Caso de uso "Programar llamadas de prueba"

3.2.1.5 Generar alertas

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador inició una o más pruebas de lazo cerrado.
Caso de éxito	1. La aplicación servidor monitorea la actividad de la PBX

Característica	Descripción
	ASTERISK. 2. La PBX recibe una llamada entrante. 3. La aplicación servidor analiza el número de identificador de llamada entrante. 4. Si la reconoce como un número nacional, envía una notificación. 5. Regresa al paso 1.
Caso alternativo	1. La aplicación servidor monitorea la actividad de la PBX ASTERISK. 2. El usuario apaga la función de monitorear la PBX.
Pos condiciones	- La aplicación vuelve a su estado de espera.

Tabla 3.9. Caso de uso "Generar alertas"

3.2.1.6 Agregar tarjeta

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos. - El administrador desea agregar una tarjeta de telefonía pre-pagada.
Caso de éxito	1. Abre el administrador de tarjetas. 2. Selecciona la opción de agregar una nueva tarjeta. 3. Ingresa los datos de la tarjeta en los campos especificados. 4. Selecciona la opción guardar tarjeta. 5. Cierra el administrador de tarjetas.
Caso alternativo	1. Abre el administrador de tarjetas. 2. Selecciona la opción de agregar una nueva tarjeta. 3. Ingresa mal los datos de la tarjeta en los campos especificados. 4. Selecciona la opción guardar tarjeta. 5. La aplicación cliente muestra un mensaje de error. 6. Regresa al paso 1.
Pos condiciones	- La aplicación cliente pregunta si los cambios deben ser guardados de forma permanente. - La aplicación regresa al menú principal.

Tabla 3.10. Caso de uso "Agregar tarjeta"

3.2.1.7 Modificar tarjeta

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y

Característica	Descripción
	contraseña correctos. - El administr ador desea actualizar la información de una tarjeta de telefonía pre-pagada que se encuentra registrada en el sistema.
Caso de éxito	1. Abre el administrador de tarjetas. 2. Selecciona la tarjeta que desea actualizar. 3. Ingresa los datos de la tarjeta que desea modificar. 4. Selecciona la opción para guardar los cambios. 5. La aplicación cliente pregunta si los cambios deben ser guardados de forma permanente.
Caso alternativo	1. Abre el administrador de tarjetas. 2. Selecciona la tarjeta que desea actualizar. 3. Ingresa datos de tarjeta incongruentes o incompletos. 4. Selecciona la opción para guardar los cambios. 5. La aplicación cliente muestra un mensaje de error. 6. Regresa al paso 2.
Pos condiciones	- La aplicación cliente pregunta si los cambios deben ser guardados de forma permanente. - La aplicación regresa al menú principal.

Tabla 3.11. Caso de uso "Modificar tarjeta"

3.2.1.8 Eliminar tarjeta

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos. - El administrador desea eliminar una tarjeta de telefonía pre-pagada que se encuentra registrada en el sistema.
Caso de éxito	1. Abre el administrador de tarjetas. 2. Selecciona la tarjeta que desea eliminar. 3. Selecciona la opción para eliminar la tarjeta. 4. Confirma la eliminación de la tarjeta seleccionada.
Pos condiciones	- La aplicación cliente pregunta si los cambios deben ser guardados de forma permanente. - La aplicación regresa al menú principal.

Tabla 3.12. Caso de uso "Eliminar tarjeta"

3.2.1.9 Consultar CDR's de ASTERISK

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y

Característica	Descripción
	contraseña correctos. - El administrador desea realizar una consulta a la base de datos de CDR's de ASTERISK.
Caso de éxito	1. Selecciona el generador de consulta de CDR's de ASTERISK. 2. Construye la búsqueda que desea realizar (Construir una búsqueda). 3. Envía la consulta de CDR's para que sea procesada.
Pos condiciones	- Se despliega la ventana de visualización de consulta con los datos obtenidos.

Tabla 3.13. Caso de uso "Consultar CDR's de ASTERISK"

3.2.1.10 Consultar los CDR's de ASTEM

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos. - El administrador desea realizar una consulta sobre las notificaciones que han sido generadas por el sistema.
Caso de éxito	1. Selecciona el generador de consultas de CDR's de ASTEM. 2. Construye la búsqueda que desea realizar (Construir una búsqueda). 3. Envía la consulta de notificaciones para que sea procesada.
Pos condiciones	- Se despliega la ventana de visualización de consulta con los datos obtenidos.

Tabla 3.14. Caso de uso "Consultar notificaciones generadas"

3.2.1.11 Construir una búsqueda

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador se encuentra generando una consulta de los registros CDR de ASTEERISK o de las notificaciones emitidas por el sistema.
Caso de éxito	1. Selecciona los campos que desea consultar. 2. Define las condiciones de búsqueda para filtrar información.
Caso alternativo	1. Selecciona los campos que desea consultar. 2. No define condiciones de búsqueda para filtrar información que nos son reconocidas por el sistema.
Pos condiciones	- La aplicación define el formato de la consulta.

Tabla 3.15. Caso de uso "Construir búsqueda"

3.2.1.12 Generar documentos en base a la información en las bases de datos

Característica	Descripción
Actores	- Administrador del sistema.
Pre condiciones	- Se ha generado la vista de visualización de consultas con los datos obtenidos de una consulta realizada.
Caso de éxito	1. Analiza los datos obtenidos por la consulta. 2. Selecciona las filas que desea conservar y elimina las filas no deseadas. 3. Genera un documento PDF con la información deseada.
Caso alternativo	1. Analiza los datos obtenidos por la consulta. 2. Cierra la ventana para realizar una nueva consulta.
Pos condiciones	- La aplicación regresa al generador de consultas.

Tabla 3.16. Caso de uso "Generar reporte de registros"

3.2.1.13 Generar datos estadísticos de las tarjetas utilizadas

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos.
Caso de éxito	*Caso 1* 1. Ingresa a la ventana de estadísticas. 2. Selecciona todas las tarjetas. 3. Define un parámetro para las estadísticas. 4. Realiza la consulta y visualiza los datos. 5. Cierra la ventada de estadísticas de tarjetas. *Caso 2* 1. Ingresa a la ventana de estadísticas. 2. Selecciona una tarjeta. 3. Define un parámetro para las estadísticas. 4. Realiza la consulta y visualiza los datos. 5. Cierra la ventada de estadísticas de tarjetas.
Pos condiciones	- La aplicación regresa al menú principal.

Tabla 3.17. Caso de uso "Consultar estado"

3.2.1.14 Configurar del sistema ASTEM

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos.

Característica	Descripción
Caso de éxito	1. Ingresa a ventana de configuración de ASTEM. 2. Modifica las configuraciones deseadas. 3. Guardar cambios realizados. 4. Cierra la ventana de configuración.
Pos condiciones	- La aplicación regresa al menú principal.

Tabla 3.18. Caso de uso "Configuración del sistema ASTEM"

3.2.1.15 Configurar ASTERISK

Característica	Descripción
Actores	- Funcionario administrador del sistema.
Pre condiciones	- El administrador ingresó al sistema con un usuario y contraseña correctos.
Caso de éxito	1. Ingresa a ventana de configuración de ASTERISK. 2. Modifica las configuraciones deseadas. 3. Guarda cambios realizados. 4. Aplica la configuración en la PBX ASTERISK. 5. Cierra la ventana de configuración.
Pos condiciones	- La aplicación regresa al menú principal.

Tabla 3.19. Caso de uso "Configurar ASTERISK"

3.2.2 DIAGRAMA DE CLASES

Como se especificó anteriormente, el software ASTEM será conformado por dos aplicaciones; cliente y servidor. La aplicación servidor se ejecuta junto a la PBX ASTERISK en un servidor LINUX, y procesa las tareas del sistema. Esta aplicación será tipo consola.

Por otro lado, la aplicación cliente contiene un entorno gráfico a través del cual el usuario accede y controla el sistema. Todas las instrucciones son enviadas desde la aplicación cliente hacia el servidor donde son procesadas. Las instrucciones pueden ser directamente ejecutadas en el servidor a través de comandos de consola.

3.2.2.1 Diagrama de clases de la aplicación servidor

La aplicación es iniciada desde una clase MAIN que contiene a las clases que levantan los servicios del sistema. La clase SrvAstem es la clase principal e instancia objetos de casi todas las demás clases, incluyendo SrvRegistros. En la

Figura 3.7 se puede observar el diagrama de clases diseñado para la aplicación servidor.

La clase SrvRegistros es paralela a la clase SrvAstem ya que su función es registrar todos los eventos que se produzcan en el sistema. Su interacción con todas las demás clases es a través de la interfaz Registro.

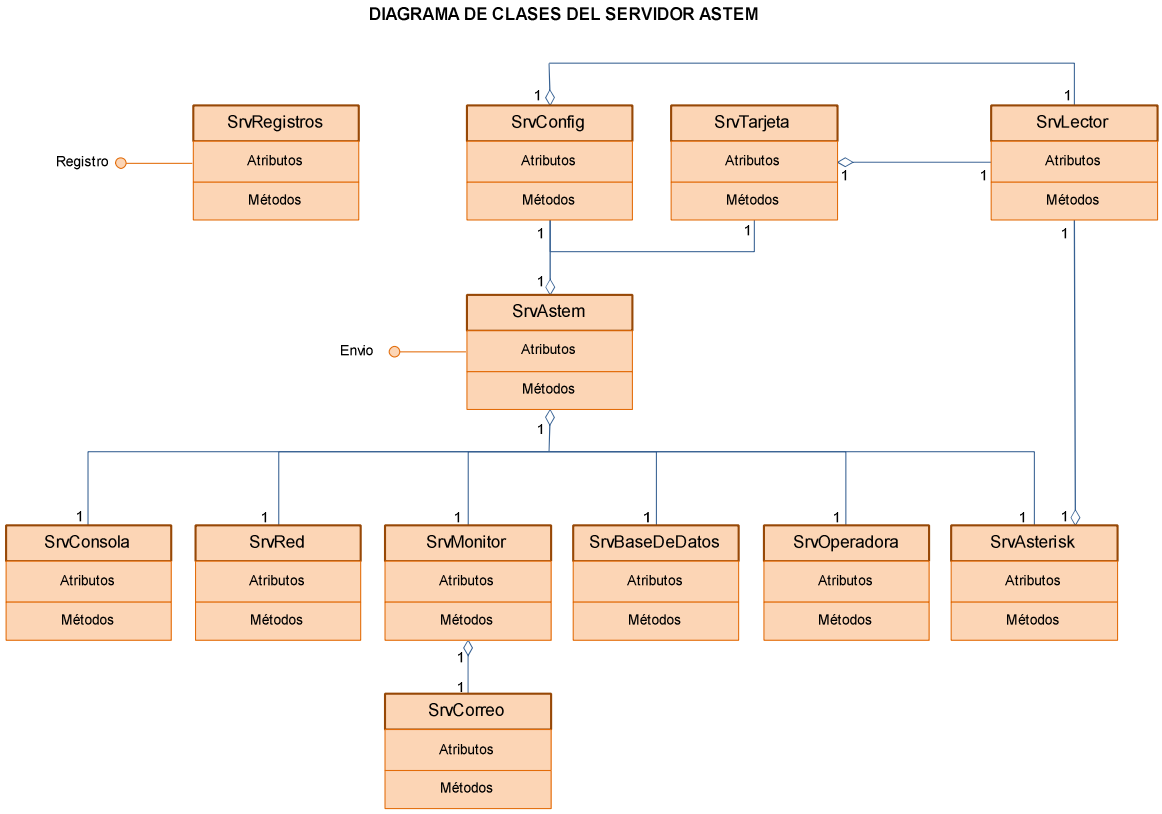


Figura 3.7. Diagrama de clases de la aplicación servidor

Las principales clases de la aplicación servidor son:

1. SrvOperadora.- Encargada de la gestión de llamadas.
2. SrvMonitor.- Encargada de monitorear la PBX ASTERISK.
3. SrvCorreo.- Encargada de enviar mensajes de correo electrónico.
4. SrvBaseDeDatos.- Encargada del acceso a las base de datos.
5. SrvConsola.- Implementa la consola del servidor ASTEM.
6. SrvRed.- Gestiona la conexión con el cliente.

7. SrvTarjeta.- Implementa la lista de tarjetas de telefonía.
8. SrvConfig.- Controla la configuración de ASTEM.
9. SrvAsterisk.- Cambia la configuración de la PBX ASTERISK.
10. SrvAstem.- Encargada de gestionar los servicios del sistema.
11. SrvRegistros.- Encargada de registrar los eventos del sistema.

3.2.2.2 Diagrama de clases de la aplicación cliente

En la Figura 3.8 se puede observar el diagrama de clases diseñado para la aplicación Cliente. La clase que inicia el entorno gráfico del programa y de la cual se derivan todas las ventanas de la aplicación es la clase ClntMenu.

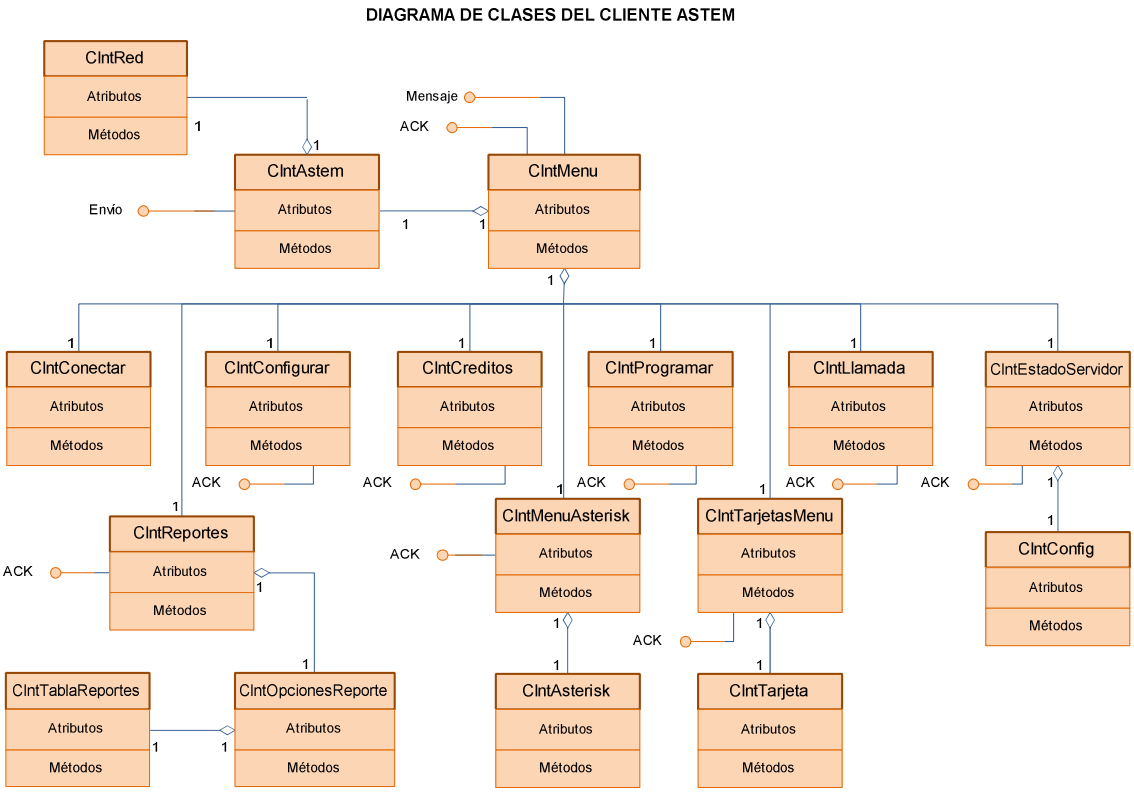


Figura 3.8. Diagrama de clases de la aplicación cliente

Las clases más relevantes de la aplicación cliente son:

1. ClntTarjeta.- Recibe la información de las tarjetas de telefonía.
2. ClntConfig.- Recibe la información de configuraciones de ASTEM.

3. ClntAsterisk.- Recibe la información de configuraciones de ASTERISK.
4. ClntRed.- Gestiona la conexión e intercambio de mensajes con el servidor.
5. ClntTablaReportes.- Recibe la información de una consulta y construye archivos PDF.
6. ClntAstem.- Administra los mensajes enviados y recibidos.
7. ClntMenu.- Crea e inicia todas las ventanas de la interfaz gráfica.
8. Ventanas y mensajes de la aplicación.- Despliegan la información recibida desde el servidor y permiten al usuario interactuar con el sistema.

3.2.3 PRINCIPALES CLASES DE LA APLICACIÓN SERVIDOR ASTEM

3.2.3.1 Clase SrvOperadora

La clase *SrvOperadora* se caracteriza principalmente por procesar las llamadas de prueba de lazo cerrado que se generen o sean programadas. Esta clase está compuesta principalmente de 3 partes. En la Figura 3.9 se observa el diagrama de actividades de la clase.

En primer lugar, esta clase depende de las clases *SrvBaseDeDatos* y *SrvOperadora* para acceder a los datos de tarjetas de telefonía y configuración de ASTEM. Estos datos son necesarios para construir los archivos que generarán las llamadas de prueba desde la PBX ASTERISK.

Cuando el servidor ASTEM recibe la instrucción para generar una llamada o un grupo de llamadas, la instancia de la clase *SrvOperadora* accede a la información de tarjetas y configuración para conocer el prefijo de llamada internacional y los códigos de las tarjetas a utilizar. Realizado esto, verifica si el valor del parámetro “disponible” en el objeto *SrvOperadora* es verdadero o falso, lo que indica si el servidor se encuentra o no realizando una prueba.

Si el objeto se encuentra disponible se lo coloca en estado de no disponible (falso) y se ejecuta un método que crea los archivos de pruebas correspondientes. Una vez creados los grupos de archivos, se ejecuta otro método que mueve las llamadas por grupos hacia la PBX ASTERISK para que

ésta las ejecute. Este método se ejecuta en un proceso paralelo que espera un tiempo determinado (tiempo definido como duración máxima de una llamada de lazo cerrado) para mover cada grupo a la cola de llamadas de la PBX. El hilo finaliza su tarea el momento en que todas las llamadas hayan sido procesadas.

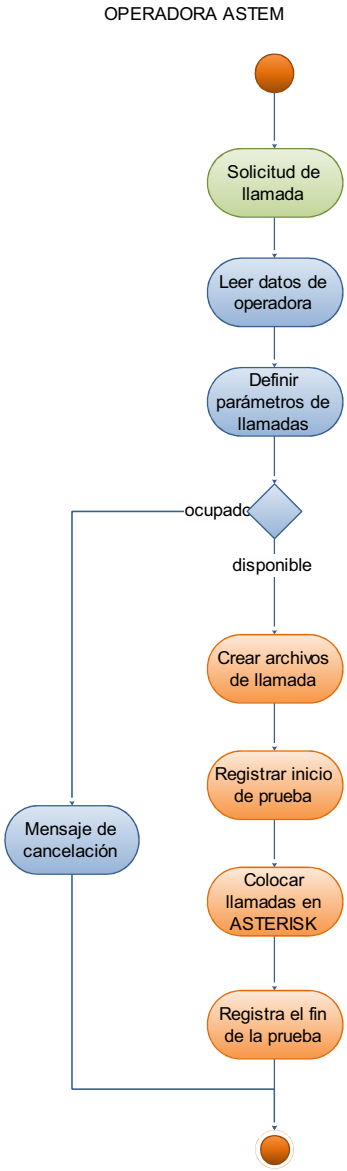


Figura 3.9. Diagrama de actividad de la clase SrvOperadora

Una vez terminado el procesamiento de llamadas, se ejecuta un método que limpia los directorios utilizados por el sistema ASTEM y se coloca al parámetro “disponible” nuevamente el valor verdadero. En la Figura 3.10 (a) se muestra un diagrama del proceso realizado por el servidor para la creación de archivos de llamada ASTERISK.

El método que genera los archivos de llamadas para la central ASTERISK inicia ordenando los parámetros principales de cada llamada, como tarjeta, troncal, destino, etc. Una vez ordenados los datos y troncales a utilizar, organiza grupos con un número definido de llamadas por grupo y crea los archivos de llamadas en una carpeta del sistema destinada a este fin.

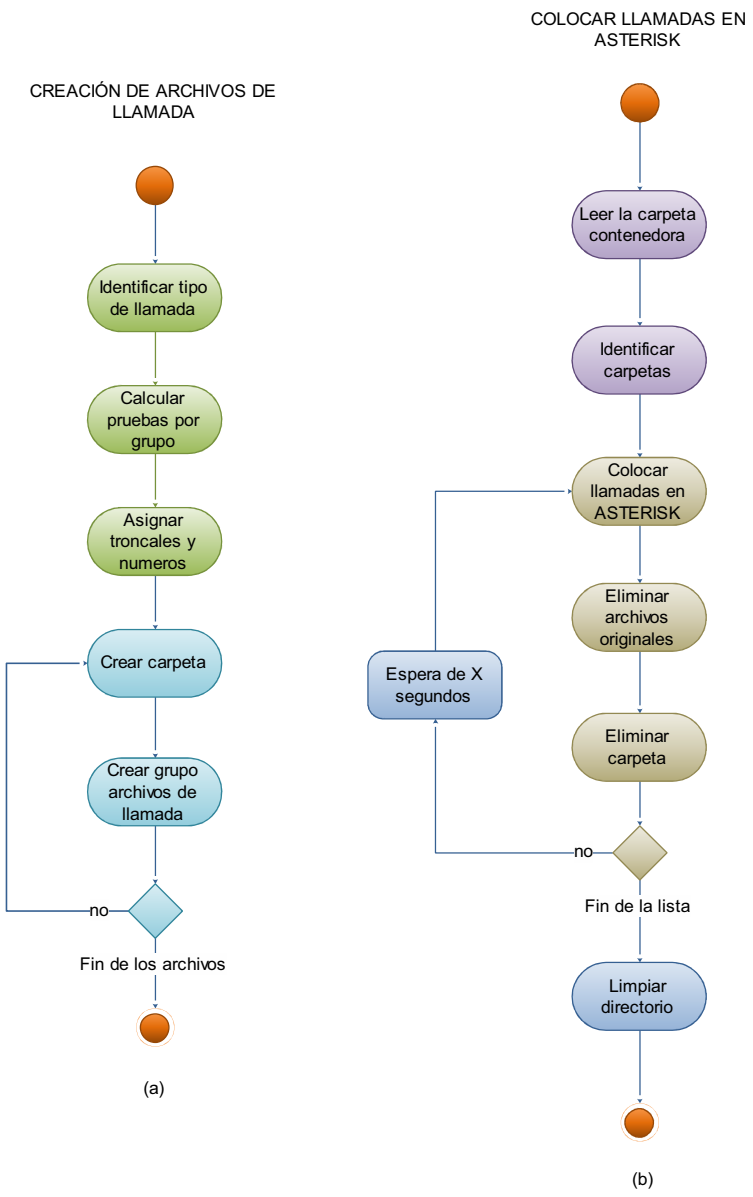


Figura 3.10. (a) Diagrama de actividades de la creación de archivos de llamada. (b) Diagrama de actividades de la generación de llamadas.

Cada grupo contiene las llamadas que la PBX debe realizar de forma simultánea. Las llamadas dentro de un grupo son organizadas de forma que cada troncal de la PBX realice una llamada a un solo destino en las troncales disponibles. De esta

manera se consigue ordenar y generar tantas llamadas de prueba simultáneas como se desee.

En la Figura 3.10 (b) se observa el proceso de generación de llamadas en la PBX. Una vez que el método ha terminado la creación de los grupos de llamadas, se ejecuta un siguiente método que lee la carpeta de archivos de llamadas de ASTEM y crea una lista de los grupos a copiar. Cada grupo contiene las llamadas que se deben realizar simultáneamente.

Luego de definir la lista, se mueven los archivos de llamadas de un grupo hacia el procesador de la PBX ASTERISK para que esta ejecute las llamadas de forma inmediata, y se agrega estas llamadas a una lista de llamadas activas en el monitor para indicarle al sistema que puertos debe monitorear. Luego, elimina el grupo de llamadas copiado y se coloca en espera un tiempo definido para posteriormente copiar el siguiente grupo de llamadas. Este proceso se repite hasta terminar de colocar todos los grupos de llamadas.

Cada vez que una llamada es procesada, se inicia un hilo paralelo que monitorea la terminación de una llamada. Luego de un tiempo máximo definido en la configuración, este hilo revisa en los registros del monitor si la llamada fue completada. Si la llamada ha sido completada termina el hilo, caso contrario, asume que ocurrió un problema durante su ejecución y elimina la llamada de la lista de llamadas activas y termina el hilo.

3.2.3.2 Clase SrvMonitor

La clase *SrvMonitor*, mediante la cual se implementa el monitor de ASTEM, tiene como función principal evaluar los *Caller ID* de las llamadas que recibe la PBX, y determinar si dichas llamadas tienen origen nacional o internacional. En la Figura 3.11 se puede observar el diagrama de actividades que realiza un objeto monitor.

Las actividades del monitor inician instanciando un objeto tipo Cliente Telnet, el cual realiza la función de conectarse con el servidor ASTERISK Manager de la PBX. Una vez establecida la sesión telnet, el servidor se autentica en la PBX y comienza a recibir los eventos producidos por su actividad. Un evento es un grupo de datos enviados por la PBX que tienen una estructura definida.

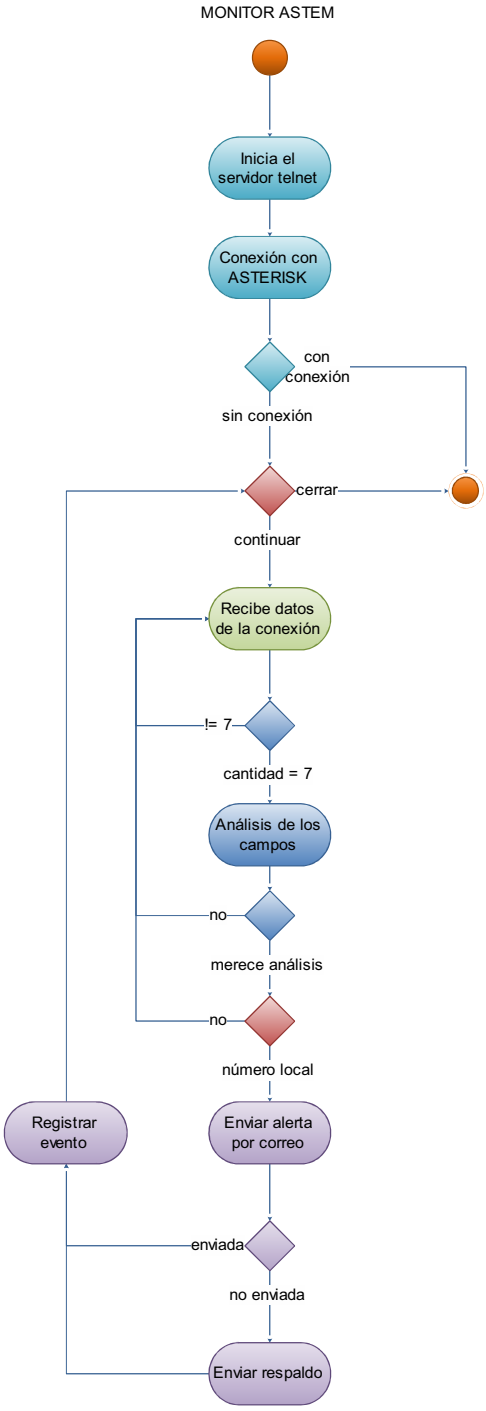


Figura 3.11. Diagrama de actividades de la clase *SrvMonitor*

Cada evento recibido a través de la conexión TELNET se analiza para verificar si corresponde a una llamada entrante. El primer análisis consiste en determinar la cantidad de parámetros que contiene el evento. Si el evento consta de 7 parámetros se procede a verificar el tipo de evento, privilegios, y actividad con el fin de determinar si se trata de una llamada entrante. En el caso de que los datos correspondan con los tipos de parámetros esperados, el siguiente paso es

comprobar que los campos *CallerID* y *CallerNameID* en el evento estén en el orden adecuado.

Una vez que un evento ha sido evaluado a través de estos filtros, se procede a extraer su *Caller ID*. El *Caller ID* se lo analiza en función de las siguientes consideraciones:

1. Contiene 9 dígitos.
2. Primer dígito 0, y el segundo dígito es 2, 3, 4, 5, 6, 7, 8 ó 9.

Si el número identificado en el *Caller ID* concuerda con los criterios de análisis, se lo considera un posible origen de fraude y se procede a generar una alerta. Dentro de la alerta se incluyen los campos *CallerID* y *UniqueID* del evento de ASTERISK, con los cuales se crea un correo electrónico de notificación. Posteriormente, un método definido utiliza un objeto de la clase *SrvCorreo* para conectar el servidor ASTEM con un servidor de correo electrónico y enviar el correo de notificación, luego se registra el CDR en la base de datos MySQL. En la base de datos se incluye un campo que indica si el correo electrónico de notificación fue enviado con éxito. Finalmente, el objeto monitor procede a analizar el siguiente evento.

La segunda función de la clase monitor es generar los CDR. Los objetos *SrvMonitor* cuentan con una lista de las llamadas activas y un temporizador que les permite calcular el tiempo máximo de cada llamada. Cuando se recibe una llamada, se verifica que esta llegue en el puerto correcto y se construye un CDR con la información almacenada en la lista de llamadas activas.

El monitor puede ser detenido en cualquier momento por el usuario. Sin embargo, al realizar una llamada de prueba o programar un grupo de llamadas, el monitor es activado automáticamente por el objeto *SrvOperadora* para que analice la actividad de la PBX. El objeto monitor se ejecuta en un hilo independiente.

3.2.3.3 Clase SrvCorreo

La clase *SrvCorreo* está diseñada para manejar la generación y envío de alertas a través de correo electrónico durante una prueba de lazo cerrado. ASTEM utiliza

dos servidores de correo, uno de ellos actúa como servidor principal y es el primero con el cual se intentará enviar las notificaciones. En caso de que exista algún problema durante la conexión o el envío del mensaje, se intenta reenviar la notificación a través del segundo servidor, siendo este un servidor de respaldo. En la Figura 3.12 se muestra el diagrama de actividades de esta clase *SrvCorreo*.

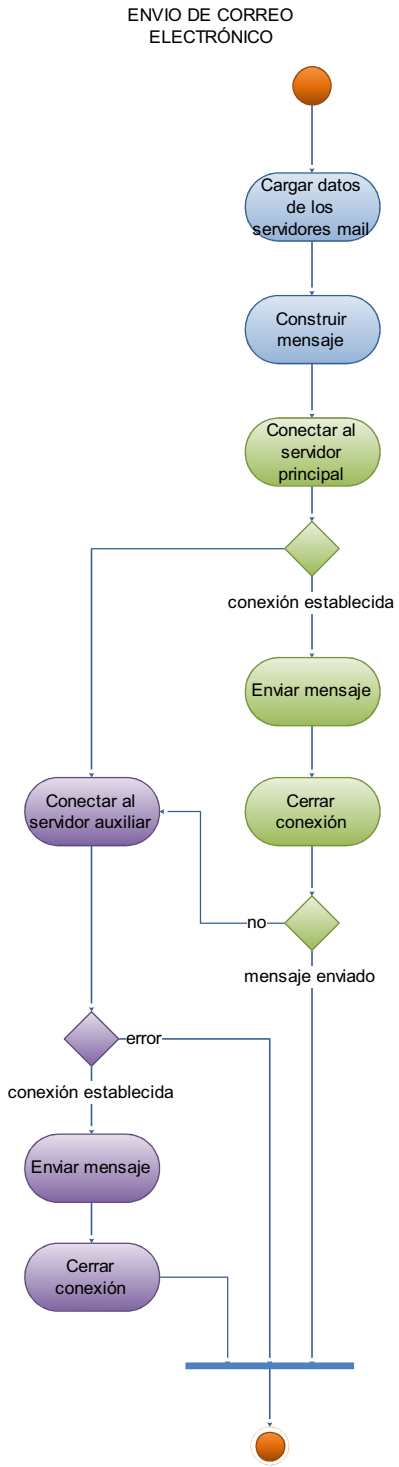


Figura 3.12. Diagrama de actividades de la clase *SrvCorreo*

Tanto la dirección destino de las alertas como las configuraciones de las cuentas de correo utilizadas por el servidor se definen en los archivos de configuración de ASTEM, y son utilizadas a través de una instancia de la clase *SrvConfig*. Los métodos en la clase *SrvCorreo* realizan la conexión a los servidores de correo electrónico y construyen el mensaje con los datos de una alerta.

Como un servicio adicional en el sistema ASTEM se incluye en la implementación un servidor de correo electrónico basado en SENDMAIL. Este servidor es instalado y ejecutado en el mismo servidor que la PBX ASTERISK y la aplicación servidor ASTEM. El servidor secundario por defecto es una cuenta de GMAIL creada para este fin. Sin embargo, para utilizar otros servidores gratuitos o propietarios se debe modificar la configuración del servidor ASTEM.

3.2.3.4 Clase SrvBaseDeDatos

La aplicación servidor ASTEM está diseñada para guardar los CDRs generados en sus llamadas en una base de datos en MySQL.

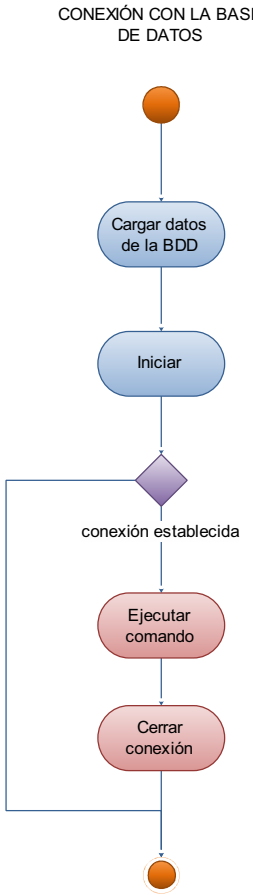


Figura 3.13. Diagrama de actividades de la clase *SrvBaseDeDatos*

La base de datos tiene 2 tablas que no se encuentran relacionadas directamente entre sí, aunque la información que guardan mantiene relación. La primera tabla es en la cual la PBX ASTERISK guarda los registros CDR's de las llamadas recibidas. La segunda tabla es en la cual ASTEM guarda los CDR's generados por las pruebas de lazo cerrado. Estos CDR's se generan en base a la información del inicio de la llamada y de fin de llamada. Los CDR's guardados por ASTEM contienen los siguientes campos:

1. Fecha de inicio.- Guarda la fecha de inicio de la prueba de lazo cerrado.
2. Fecha de fin.- Guarda la fecha en que se recibió la prueba de lazo cerrado. Este campo puede quedar en blanco cuando se realizan las llamadas de prueba a números que no están conectados a la PBX.
3. Origen.- Guarda el número que originó la llamada de prueba.
4. Destino.- Guarda el número al que se marcó en la llamada de prueba.
5. CallerID.- Guarda el *CallerID* recibido en una llamada de prueba. Este campo puede quedar en blanco cuando se realizan las llamadas de prueba a números que no están conectados a la PBX.
6. Duración.- Guarda el tiempo facturable de la llamada de prueba.
7. Tarjeta.- Guarda el nombre de la tarjeta utilizada para la prueba.
8. Alerta.- Guarda un 1 si el *Caller ID* fue identificado como sospechoso, caso contrario almacena 0.
9. Mail.- Guarda un 1 si se envió una alerta, caso contrario 0.
10. IDSaliente.- Guarda el identificador del CDR ASTERISK de la llamada que originó la prueba de lazo.
11. IDEntrante.- Guarda el identificador del CDR ASTERISK de la llamada que recibió la prueba de lazo. Guarda el identificador del CDR ASTERISK de la llamada que originó la prueba de lazo.

12. Contestada.- Guarda un 1 si la llamada fue contestada en la PBX, caso contrario 0.

13. Usuario.- Campo reservado para futuras aplicaciones.

La clase *SrvBaseDeDatos* implementa métodos para conectar al servidor ASTEM con la base de datos en MySQL. En la Figura 3.13 se puede observar las actividades definidas en los métodos de la clase *SrvBaseDeDatos* para actualizar o consultar una tabla de la base. Es importante mencionar que el sistema ASTEM no modifica la tabla de CDR's de ASTERISK, únicamente la lee.

El proceso inicia con el método que realiza la conexión con la base de datos. Si la conexión es exitosa, la instancia de la clase ejecuta un comando especificado sobre la tabla correspondiente y devuelve el resultado de la operación, de ser el caso, al objeto que lo solicitó. Por último, se cierra la conexión con la base de datos. Este proceso se realiza cada vez que es necesario efectuar una consulta o actualizar una tabla.

Los parámetros de acceso a la base de datos son definidos en los archivos de configuración de ASTEM y pueden ser modificados a través del cliente ASTEM.

3.2.3.5 Clase SrvConsola

La consola del servidor ASTEM es la interfaz a través de la cual el servidor ASTEM recibe instrucciones locales. En la Figura 3.14 se muestra el diagrama de actividades definidas en la clase *SrvConsola*.

La clase *SrvConsola* es instanciada dentro de la clase *SrvAstem* y ejecuta sus actividades desde que inicia la aplicación servidor ASTEM, y se detiene cuando el programa es cerrado. Se ejecuta como un servicio paralelo en un hilo independiente y su función es recibir instrucciones para que el servidor las ejecute.

Cuando el método de la consola ha iniciado, se escribe un "prompt" en pantalla y se coloca en estado de espera hasta que el usuario ingrese un comando por teclado. Los comandos se leen una vez que se presiona la tecla "ENTER". Una vez recibido un comando por consola, se lo codifica y envía al hilo principal del

programa para que sea procesado. Finalmente, el método en la clase *SrvConsola* vuelve al estado de espera.

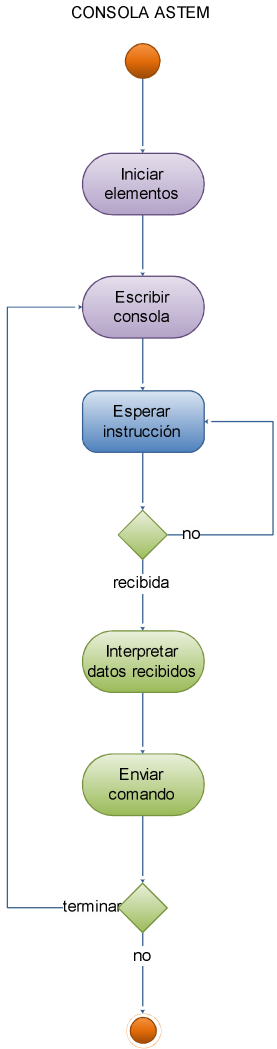


Figura 3.14. Diagrama de actividades de la clase *SrvConsola*

3.2.3.6 Clase SrvRed

ASTEM es una aplicación distribuida por lo que las actividades especificadas en esta clase son de extrema importancia para su correcto funcionamiento. Los servicios de red del servidor gestionan la comunicación con el usuario que se conecta de forma remota utilizando la aplicación cliente.

La clase *SrvRed* es instanciada en la clase principal *SrvAstem* al iniciar el servidor. Las actividades descritas en sus métodos se inician en un hilo paralelo junto con el proceso principal de la aplicación servidor ASTEM. La Figura 3.15 muestra el diagrama de actividades de la clase *SrvRed*. En cuanto el servidor

ASTEM ha iniciado, la instancia de *SrvRed* abre el puerto especificado para recibir conexiones y lo escucha a la espera de una conexión TCP. Se escogió TCP por ser un protocolo orientado a conexión que ofrece mayor confiabilidad en la transmisión de datos.

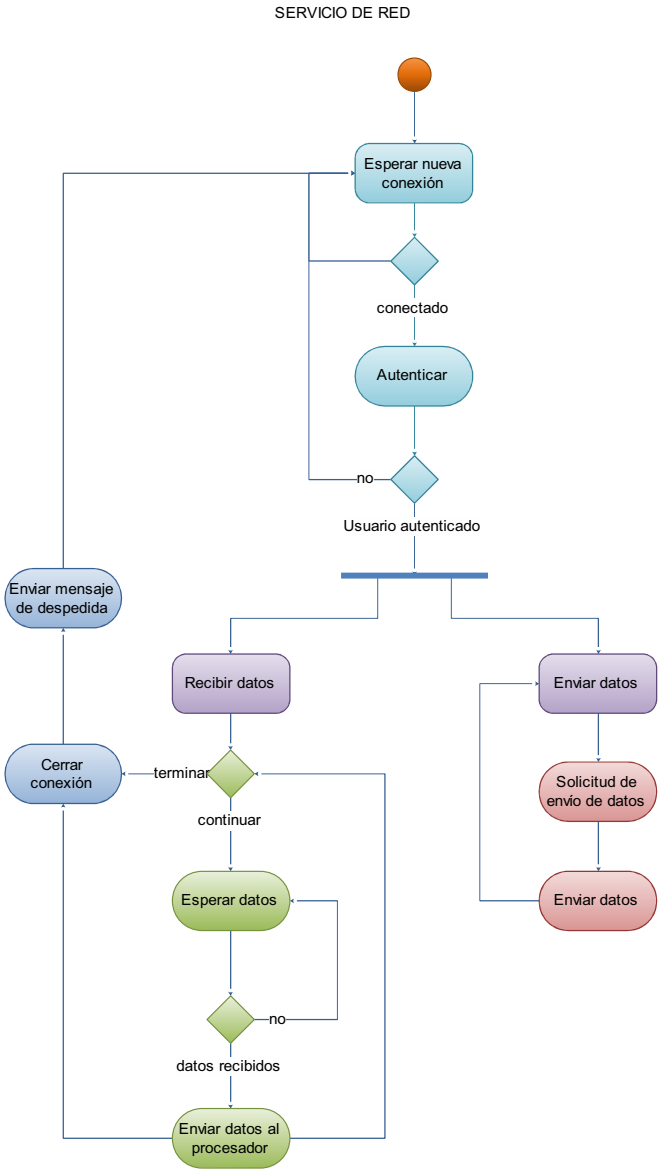


Figura 3.15. Diagrama de actividades de la clase *SrvRed*

Cuando una conexión es recibida, se asigna un socket para dicha conexión y el cliente entra en la etapa de autenticación de usuario. El servidor espera hasta recibir un mensaje de solicitud de autenticación desde el cliente. Una vez recibida la cadena correcta, el método encargado de la autenticación responde enviando un reto, el cual consiste en un número que es utilizado para codificar la contraseña del usuario en la aplicación cliente.

Una vez que la aplicación cliente recibe el reto, esta lo resuelve utilizando los datos de usuario y contraseña ingresados por el usuario. La solución al reto es enviada al servidor el cual la compara con la solución generada en base a sus datos. Si las soluciones coinciden, el método de autenticación devuelve un resultado positivo con el cual da acceso al cliente y éste puede comenzar a enviar instrucciones. El objeto *SrvRed* se coloca en estado de escucha para recibir datos a través de la conexión y coloca en modo de espera a cualquier otra conexión que se desee establecer. En la Figura 3.16 se puede observar el diagrama de las actividades definidas en la clase *SrvRed*.

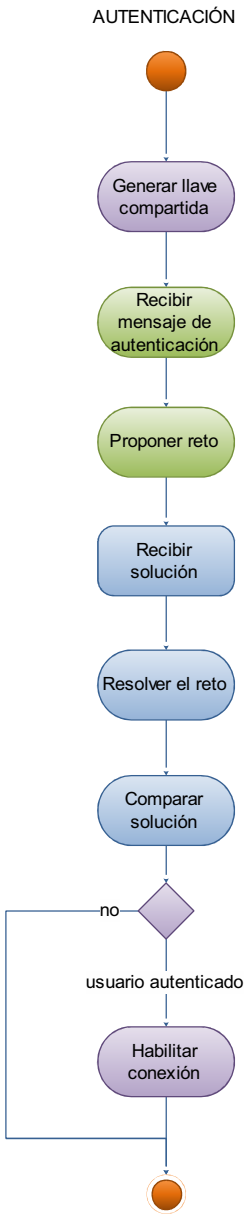


Figura 3.16. Diagrama de actividades del proceso de autenticación

Cuando se establece la conexión con un cliente, y luego de la autenticación, se inician dos hilos. El primero cumple la funcionalidad de recibir la información enviada desde cliente, y se ejecutada como un hilo independiente. Este hilo contiene un lazo infinito que escucha la conexión y recibe datos mientras la conexión esté activa. Los datos recibidos son enviados al hilo principal del programa para que sean procesados en el método correspondiente. El segundo hilo tiene la función de enviar mensajes de respuesta al cliente. Las actividades de este hilo se ejecutan desde el objeto *SrvRed*, por lo cual pueden ser iniciadas en cualquier momento sin interrumpir el hilo de recepción de mensajes.

Para cerrar la conexión se utiliza señalización de 2 vías y solo el cliente puede iniciar el proceso de desconexión. En el primer mensaje, el cliente indica al servidor que desea cerrar la conexión. Al recibir la instrucción de desconexión, el servidor la procesa y responde afirmativamente a través de un mensaje de despedida, luego se detiene el método de escucha de mensajes. Una vez terminada una conexión, el servidor cierra el socket utilizado y vuelve a su estado de escucha de nuevas conexiones.

3.2.3.7 Clase SrvTarjeta

Las actividades definidas para esta clase corresponden a la administración de la información de las tarjetas de telefonía pre-pagada almacenadas en el servidor. Esta información es utilizada por la clase *SrvOperadora* cuando crea archivos de llamada. Dichos archivos de llamada son utilizados para definir las opciones utilizadas por la IVR de la PBX ASTERISK.

Las tarjetas son almacenadas en el servidor ASTEM utilizando un archivo de configuración de tarjetas llamado “tarjeta.astem”. La clase *SrvTarjeta* construye objetos que contienen los datos de las tarjetas como variables.

Al iniciar la aplicación servidor ASTEM, el método constructor lee el archivo de tarjetas utilizando una instancia de la clase *SrvLector* y crea una lista con objetos que contienen los datos leídos. La clase *SrvTarjeta* define métodos que actualizan los datos de las tarjetas o codifican la información almacenada para que pueda ser enviada al cliente.

3.2.3.8 Clase SrvConfig

La clase *SrvConfig* define métodos para administrar las configuraciones utilizadas en el servidor ASTEM. La aplicación servidor maneja un grupo de configuraciones que van desde el puerto en el que escucha conexiones provenientes de los clientes, hasta los detalles de los servidores utilizados para enviar notificaciones. Los aspectos configurables en el servidor ASTEM son:

- Parámetros de conexión al servidor ASTEM.
- Parámetros del generador de llamadas.
- Parámetros del monitor de la PBX ASTERISK.
- Parámetros de la base de datos MySQL y las tablas utilizadas.
- Parámetros de las direcciones de correo utilizadas para enviar las alertas.
- Parámetros de los usuarios del sistema ASTEM.
- Troncales y números configurados en el servidor ASTERISK.

Con excepción de los datos de usuarios, los parámetros de configuración están contenidos en el archivo “admin.astem”. La estructura de este archivo es utilizando etiquetas, donde cada etiqueta representa un grupo de parámetros de configuración que la aplicación servidor ASTEM interpreta. Las etiquetas se definen entre corchetes ([*etiqueta*]), y todos los parámetros configurados debajo de una etiqueta pertenecen al mismo grupo hasta que se encuentre otra etiqueta o se alcance el final del archivo. Todos los parámetros se configuran con el formato “<parámetro>=<valor>”.

La información de los usuarios de la aplicación ASTEM está guardada en el archivo “usuarios.astem”. Este archivo maneja una sintaxis similar a la del archivo de configuración principal, sin embargo en este archivo los corchetes contienen el nombre de usuario ([idusuario]), y la contraseña debe estar en la siguiente línea con el formato “clave=<contraseña>”.

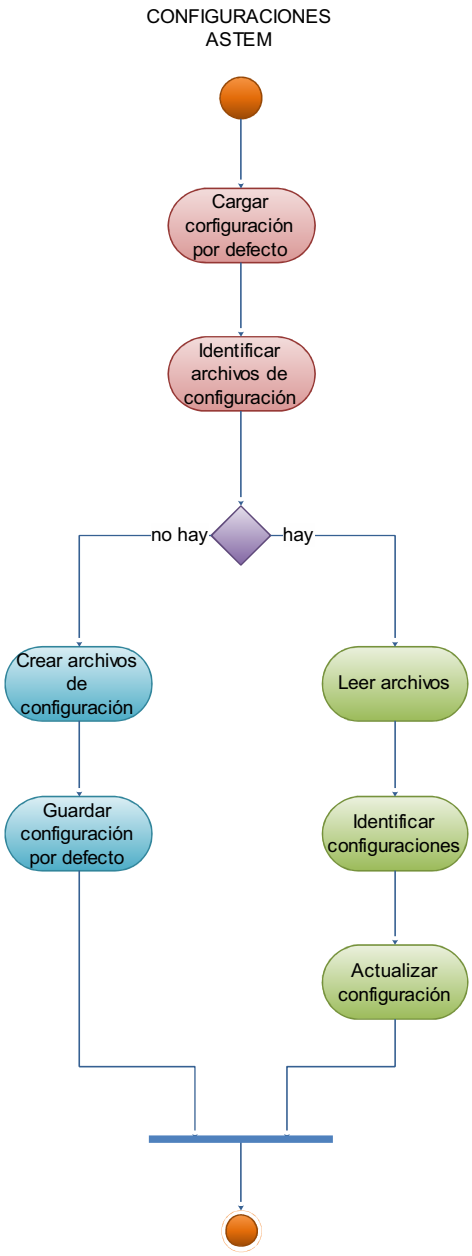


Figura 3.17. Diagrama de actividades al leer los archivos de configuración

En la Figura 3.17 se puede observar el diagrama de actividades que realiza un objeto *SrvConfig* al leer los archivos de configuración. Antes de iniciar el servicio ASTEM, el programa instancia un objeto de la clase *SrvConfig* y carga las configuraciones por defecto. A continuación, lee los archivos de configuración y actualiza los parámetros que hayan sido definidos. En caso de no encontrar o interpretar un campo dentro de los grupos de configuración, mantiene la configuración por defecto. En caso de no encontrar archivos de configuración, los crea con la configuración por defecto.

3.2.3.9 Clase SrvAsterisk

La clase *SrvAsterisk* define métodos que permiten leer la configuración de la PBX ASTERISK, actualizarla, y reiniciar la PBX para que los cambios realizados en la configuración sean aplicados. Una instancia de esta clase es utilizada cuando el cliente desea realizar cambios en la configuración de la PBX.

El servidor ASTEM únicamente permite configurar los parámetros correspondientes a las funciones que cumple la PBX ASTERISK. Los archivos de configuración que permite modificar son “extensions.conf”, “sip.conf”, “manager.conf”, y “cdr_mysql.conf”.

3.2.3.10 Clase SrvRegistros

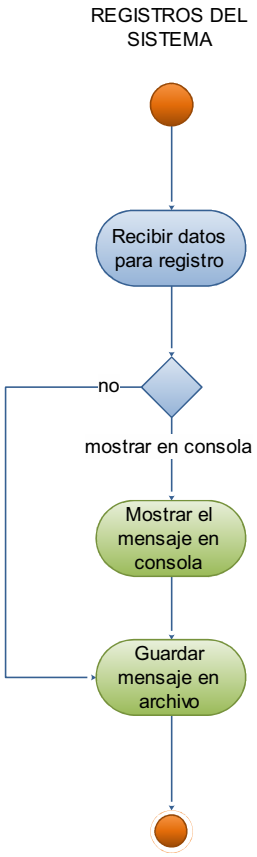


Figura 3.18. Diagrama de actividades de la clase *SrvRegistros*

En todo programa es importante que exista un registro detallado de las tareas que realiza la aplicación y los errores o fallas que se generen. Para realizar esta tarea se ha diseñado la clase *SrvRegistros* la cual implementa métodos que registran la actividad y mensajes que se producen en el sistema.

En la Figura 3.18 se puede observar el diagrama de actividades que realizan los métodos de la clase *SrvRegistros* para registrar un evento en los logs del sistema. Cuando se ejecuta un proceso específico en el servidor, se genera un mensaje que puede ser de información, error o respuesta a una instrucción. Estos mensajes son registrados en el archivo “astemlog” en la carpeta “/var/log/” junto con la fecha y hora en que se originó.

Esta clase es instanciada antes de la clase principal del sistema, y recibe la información a registrar a través de la interfaz *InterfazRegistros*. Los mensajes que recibe son guardados en el archivo de registros. Si la publicación de mensajes en consola está activa (DEBUG), los mensajes también son publicados en consola.

3.2.3.11 Clase SrvAstem

La clase *SrvAstem* es la clase principal de la aplicación servidor ASTEM y desde donde se ejecutan todos los servicios. En esta clase se implementan métodos para procesar las instrucciones recibidas.

En primer lugar el programa carga las configuraciones utilizando objetos *SrvTarjeta* y *SrvConfig*, e inicia el registro del sistema. Una vez hecho esto, el programa instancia un objeto de la clase *SrvAstem*, el cual inicia los servicios de red, consola, y monitor para luego colocarse en espera de una instrucción. Este método se ejecuta hasta recibir la instrucción de finalización del programa. En la Figura 3.19 se puede observar el diagrama de actividades que realiza el método principal de la aplicación servidor para iniciar los servicios desde un objeto *SrvAstem*.

La instrucción de terminación del programa solo puede ser ejecutada vía consola en el servidor, es decir, el servidor ASTEM no puede ser detenido por un usuario conectado a través de la aplicación cliente. Esto con el fin de garantizar que el servicio no sea detenido de forma remota.

El método que procesa las instrucciones es el núcleo del servidor ya que su función es identificar toda instrucción con sus parámetros para luego procesarla. En la Figura 3.20 (a) se observa un diagrama de actividades que se llevan a cabo en el método procesador de instrucciones.

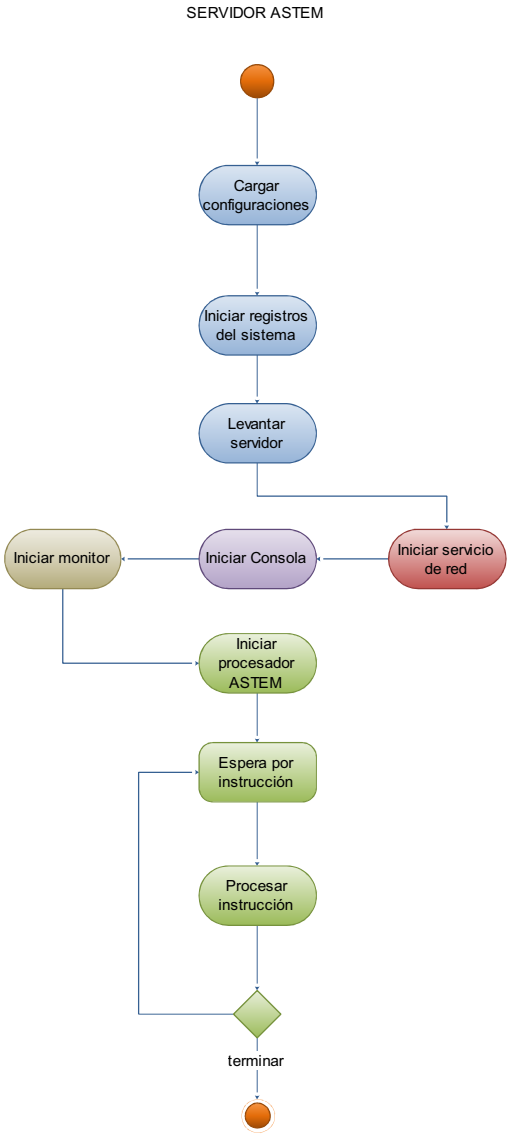


Figura 3.19. Diagrama de actividades en la clase *SrvAstem*

En primer lugar, el procesador separa los datos recibidos e identifica el tipo de función solicitada, elije la acción adecuada y procesa la función. Una vez terminado el proceso, los resultados son enviados al método procesador de respuestas y termina el proceso.

El servidor ASTEM reconoce como comandos las siguientes palabras clave. Cada instrucción tiene sus parámetros de funcionamiento:

- *llamar*
- *tarjeta*
- *consulta*

- *astem*
- *asterisk*
- *cronograma*
- *estado*
- *debug (solo por consola)*
- *desconectar (solo por red)*
- *quit (solo por consola)*

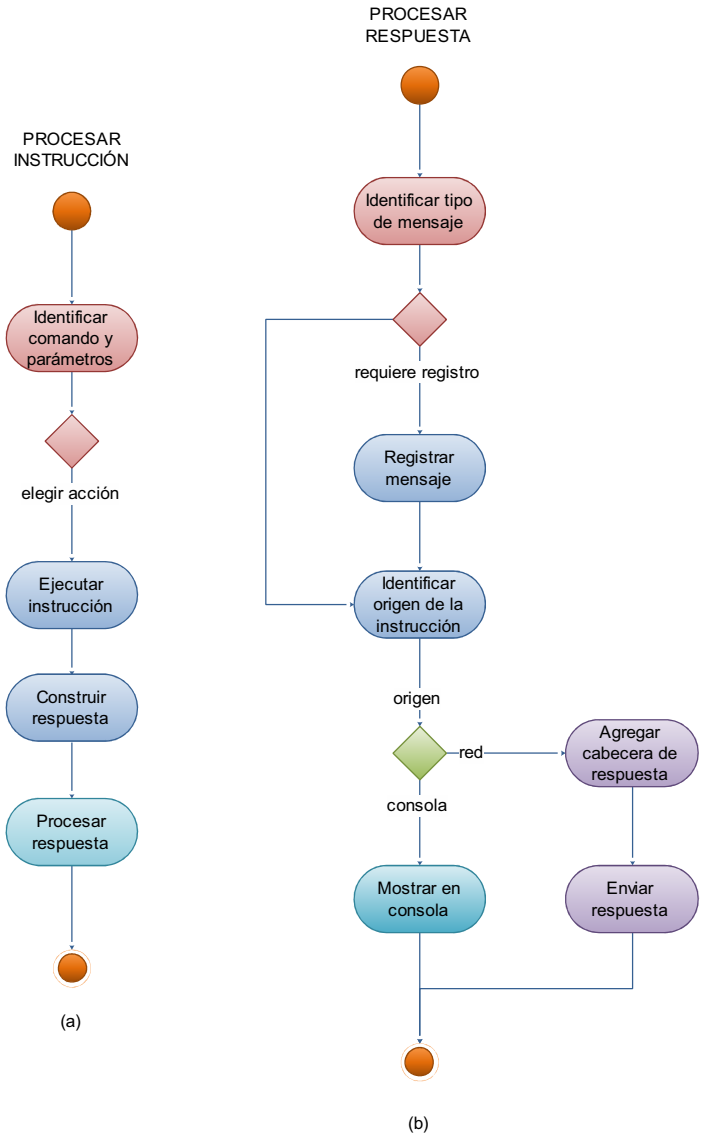


Figura 3.20. (a) Diagrama de actividades del procesador de instrucciones. (b) Diagrama de actividades del proceso de respuesta.

En la Figura 3.20 (b) se puede observar el diagrama de actividades en el método procesador de respuestas. En este método primero se identifica el tipo de respuesta que se va a procesar; con esta información se determina si la respuesta debe ser registrada como parte de los registros del sistema. En algunos casos, como en una consulta a bases de datos, esta información no debe ser considerada como mensajes para los registros del sistema.

En segundo lugar se identifica si la instrucción provino de un cliente remoto o si fue ingresado a través de consola. Según el origen, si la instrucción es local (consola) se procede a publicar la respuesta por consola; si es remota, se agrega la cabecera correspondiente al mensaje y se lo envía a través de la conexión utilizando el objetivo tipo *SrvRed*.

3.2.4 PRINCIPALES CLASES DE LA APLICACIÓN CLIENTE ASTEM

3.2.4.1 Clase ClntTarjeta

El manejo de toda la configuración del sistema ASTEM está en los archivos de configuración en el servidor,. Sin embargo, para facilidad del usuario se ha implementado la opción de configurar estos archivos a través del entorno gráfico que la aplicación cliente ofrece.

La clase *ClntTarjeta* instancia un objeto que recibe la información de las tarjetas de telefonía configuradas en el servidor. El objeto tiene métodos que codifican la información para transmitirla, y decodifican la información recibida desde el servidor. También realiza los cambios o actualizaciones indicados por el usuario a través de la ventana de configuración.

La estructura de esta clase está basada en la clase *SrvTarjeta*.

3.2.4.2 Clase ClntConfig

Similar a las funciones de la clase *ClntTarjeta*, la clase *ClntConfig* define atributos y métodos que permiten mostrar y actualizar la configuración del sistema ASTEM. Un objeto de esta clase recibe los datos de configuración desde el servidor y los decodifica para que sean mostrados en la ventana de configuración.

También se definen métodos que permiten actualizar los valores de configuración. De igual forma, contiene métodos que codifican los datos de configuración para que sean enviados al servidor para su actualización. Esta clase está basada en la estructura de la clase *SrvConfig*.

3.2.4.3 Clase ClntAsterisk

La clase *ClntAsterisk* está diseñada para manejar la información de configuración de la PBX ASTERISK que es recibida desde el servidor ASTEM. Además, esta clase define atributos y métodos que realizan la decodificación de la información recibida y codificación de la información a enviar.

3.2.4.4 Clase ClntRed

La clase *ClntRed* define métodos que administran la conexión con el servidor, similar a la clase *SrvRed* de la aplicación servidor ASTEM. El método para recibir mensajes envía la información recibida a una interfaz para que sea dirigida a la ventana correspondiente. La clase *ClntRed* también inicia el proceso de conexión y autenticación con el servidor utilizando los datos ingresados por el usuario.

Una vez establecida la conexión con el servidor, se envía el mensaje de solicitud de autenticación y espera la respuesta del servidor con el reto. Recibido el reto, codifica la respuesta utilizando los datos recibidos y la envía de vuelta al servidor. Si la aplicación cliente recibe un mensaje de confirmación afirmativo luego de la autenticación, habilita las opciones de la aplicación cliente.

A diferencia de la aplicación servidor, todas las actividades de la clase *SrvRed* se ejecutan en un proceso paralelo. Los procesos que utilizan métodos de un objeto de esta clase se comunican con él a través de una interfaz. Esto es necesario en la aplicación cliente ya que el entorno gráfico se ejecuta sobre el proceso principal.

Si el usuario selecciona la opción de desconexión, la aplicación cliente envía el mensaje de desconexión al servidor y espera un último mensaje a través de la conexión. Una vez recibida la confirmación (mensaje de despedida) termina el proceso y bloquea las opciones de la aplicación cliente.

3.2.4.5 Clase ClntReportes

La clase *ClntReportes* permite realizar consultas a la base de datos de ASTERISK y de ASTEM. La consulta puede ser construida utilizando las opciones en la ventana de forma sencilla. Para visualizar la información recibida, la clase se instancia la clase *ClntTablaReportes*, la cual permite visualizar los datos de una consulta realizada. Además, la clase *ClntTablaReportes* define funciones que permiten revisar la información de una consulta y guardar los datos en un documento PDF u hoja de cálculo. El método que realiza la consulta se encuentra especificado en la clase *ClntReportes*.

La generación de documentos se la realiza en dos etapas. En la primera se ejecuta una consulta sobre la base de datos y se obtienen los resultados, los cuales son publicados en una tabla. El usuario puede eliminar filas de esta tabla y seleccionar únicamente aquella información que es de interés. Finalmente, a través del menú se puede generar un archivo PDF o una hoja de cálculo con la información contenida en la tabla.

Para la construcción del documento esta clase utiliza un API de JAVA llamado iText. Este API contiene los métodos necesarios para esta tarea.

3.2.4.6 Clase ClntAstem

La clase *ClntAstem* instancia un objeto tipo *ClntRed*, y cumple la función de comunicar las ventanas de la aplicación cliente con el objeto *ClntRed* para utilizar los métodos de envío y recepción de mensajes.

Las instrucciones al servidor son originadas en las ventanas de la aplicación. La clase *ClntAstem* no contiene métodos que ejecuten una instrucción o procesen una respuesta. Los métodos definidos en esta clase permiten la comunicación entre los diferentes procesos y ventanas de la aplicación cliente. Cuando una ventana es abierta, esta pasa a recibir todos los mensajes que se reciban por red para que los procese. Al cerrar esta ventana, el control regresa al objeto *ClntAstem*.

Cuando una respuesta es recibida desde el servidor es enviada hacia la ventana que se encuentre recibiendo respuestas a través de la interfaz InterfazACK. El

procesamiento de cada instrucción y respuesta del servidor se realiza en la ventana activa.

3.2.4.7 Clase ClntMenu

La clase ClntMenu construye la ventana principal de la aplicación cliente. Cuando el programa inicia, se instancia un objeto tipo ClntMenu que dibuja la ventana principal. Esta clase está diseñada en base a las bibliotecas Swing y es la clase padre de prácticamente todas las ventanas del programa.

3.2.4.8 Ventanas y mensajes de la aplicación

Cada ventana de la aplicación es una instancia de una clase Swing de JAVA. El grupo de ventanas de la aplicación tiene un orden jerárquico en la estructura de las clases Swing.

En la parte superior de esta jerarquía se encuentran un objeto JFrame, que en otras palabras es la ventana principal del programa (*ClntMenu* es un objeto JFrame). El JFrame en Java es un objeto considerado como “padre” del cual pueden derivar otros objetos (ventanas) como el JDialog. Cada ventana de trabajo de la aplicación está diseñada sobre un JDialog que tiene como proceso padre al JFrame principal, o a otro JDialog. Esto objetos son iniciados y ejecutados en el JFrame. En la Figura 3.21 se puede observar la jerarquía que tienen las ventanas (objetos) que utiliza el usuario para manejar el sistema.

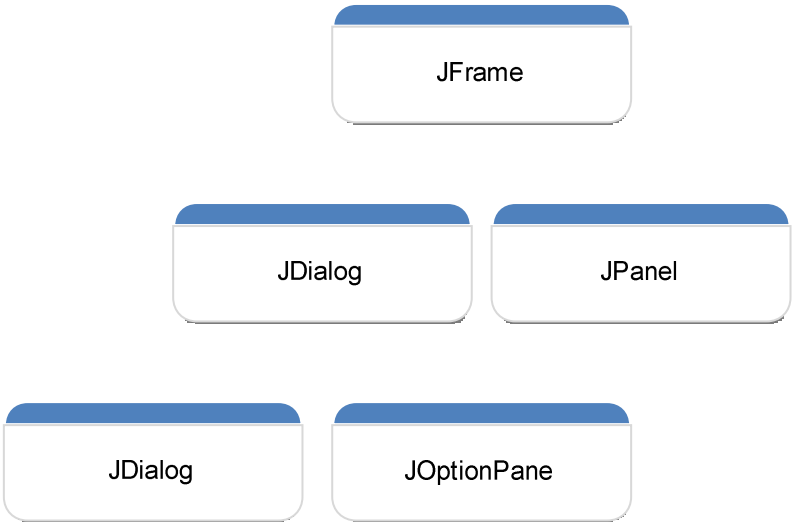


Figura 3.21. Jerarquía de los objetos gráficos de la aplicación cliente

Una de las ventajas de esta estructura es que se puede definir para que el objeto que nace del JFrame (objeto hijo) bloquee la actividad del objeto padre (JFrame o JDialog) hasta que termine sus funciones. Esto permite manejar varias ventanas de forma controlada.

Los mensajes de aviso de la aplicación cliente se muestran a través de una clase definida en JAVA Swing, la cual contiene diferentes tipos de cuadros de diálogo para mostrar mensajes. Esto facilita el trabajo de forma que es posible utilizar cuadros de diálogo de error, información o pregunta para mostrar directamente un mensaje al usuario.

A diferencia del servidor, la aplicación cliente procesa las instrucciones en diferentes ventanas, dependiendo de la ventana activa. Esto debido a que cada instrucción tiene asociado al menos una ventana para el usuario. A través de esta ventana el usuario selecciona las opciones que el programa luego codifica como instrucciones para entonces enviarlas al servidor. De igual forma, al recibir un mensaje de respuesta desde el servidor, este mensaje es procesado por la ventana que se encuentra activa en ese momento.

Para recibir los mensajes desde el servidor, se utiliza una interfaz que está definida en todas las ventanas de la aplicación. Cuando una ventana es activada, ésta pasa a controlar la interfaz de recepción de mensajes y recibe mensajes desde el servidor mientras se encuentre activa. Esta funcionalidad le permite intercambiar mensajes con el servidor. En otras palabras, si se trabaja en la ventana de configuraciones de ASTEM, esta ventana únicamente interpreta los mensajes que corresponden a mensajes de configuración. Cualquier otro mensaje recibido es publicado como aviso y no realizará ninguna acción.

Prácticamente todas las ventanas de la aplicación cliente necesitan información del servidor para mostrarla al usuario. Esta información es solicitada el momento de crear el objeto que dibuja la ventana. Al recibir la información, la ventana se actualiza mostrando al usuario los datos correspondientes. En la Figura 3.22 se observa como ejemplo la ventana de configuraciones. Esta ventana muestra los datos de configuración del sistema recibidos desde el servidor.

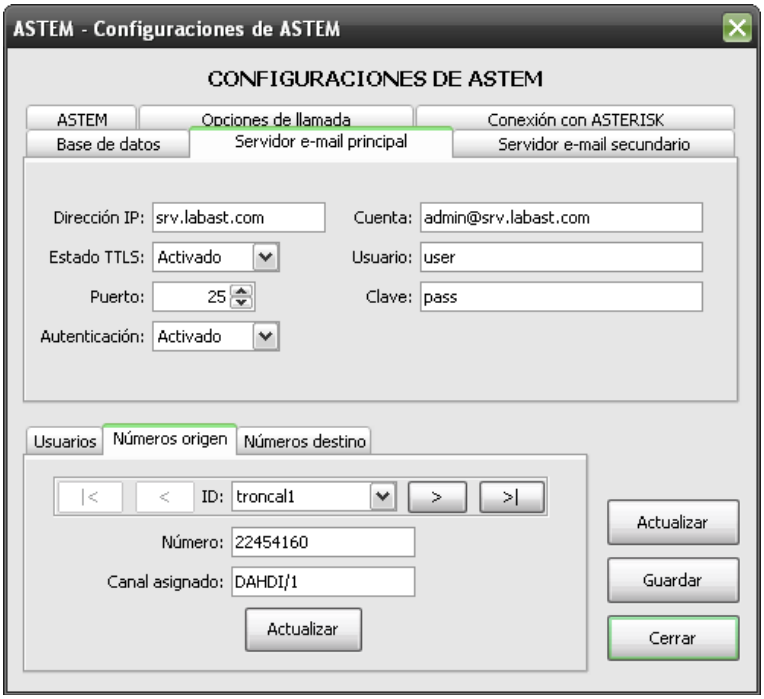


Figura 3.22. Ventana de configuración de ASTEM

3.2.5 FUNCIONAMIENTO DE LA CENTRAL TELEFÓNICA ASTERISK

Como se analizó en el apartado anterior, el gestor de llamadas del sistema está constituido por una central telefónica ASTERISK. El tener una central telefónica brinda varias ventajas en la implementación de este sistema, entre las que podemos destacar la facilidad de generación automática de llamadas.

Este aspecto tiene una singular importancia ya que el programa servidor ASTEM lo utiliza para poner en marcha las pruebas que se desee realizar. En una central telefónica ASTERISK, o PBX ASTERISK, existen principalmente dos métodos para generar llamadas.

- Archivos de llamadas.- Este método consiste en crear archivos con extensión “.call” que son reconocidos por ASTERISK para generar llamadas automáticamente. Estos archivos son colocados en la carpeta “/var/spool/asterisk/outgoing”, donde ASTERISK los procesa prácticamente de forma inmediata.

- Comandos de llamada.- Este método utiliza la conexión a ASTERISK a través del puerto de administración, para enviar comando específicos que ASTERISK utiliza para generar las llamadas.

En ambos casos se deben definir parámetros como la troncal a utilizar en cada llamada y la extensión con la que se conectará una llamada de ser contestada. Esta funcionalidad de la central facilita la implementación del sistema ya que a través de esta conexión, se conectará con una serie de comandos que lleven a cabo la llamada de lazo cerrado.

Para este trabajo se utilizará el método de generación de archivos de llamada. Como se mencionó en el módulo gestor de llamadas, el servidor ASTEM generará los archivos con los parámetros adecuados para luego colocarlos en grupos en la carpeta de ASTERISK y que sean procesados.

Con el fin de que la PBX ASTERISK cumpla con las funcionalidades deseadas, su configuración debe concentrarse en 4 aspectos principales:

1. Plan de marcación.
2. Configuración de troncales.
3. Configuración de usuarios.
4. Configuración de CDR's.

3.2.5.1 Plan de marcación

El plan de marcación es, sin duda, el elemento más importante a configurar ya que es aquí donde las extensiones y los procesos para una llamada de prueba se llevarán a cabo, tanto para recibir como para generar llamadas.

El plan de marcación contenido en el archivo “extensions.conf” debe especificar por lo menos 2 contextos. El primero será para realizar los procedimientos necesarios y llevar a cabo la llamada de prueba, mientras que el segundo será encargado de recibir las llamadas de prueba. Por motivos de seguridad, no se habilitará en el plan de marcación ningún tipo de llamada desde la central hacia el exterior.

3.2.5.2 Configuración de troncales

La configuración de las troncales a utilizar determinará el camino que utilicen las llamadas de prueba para ingresar o salir. Esta configuración debe estar contenida

en el archivo “sip.conf” si se trabaja con protocolo SIP, “iax.conf” si se trabaja con el protocolo IAX2, o en el archivo “chan_dahdi.conf” si se trabaja con tarjetas de telefonía.

Ya que la central telefónica no estará disponible para realizar llamadas que no sean de lazo cerrado, no se configura extensiones en la misma, lo cual además brinda un componente de seguridad adicional. En este trabajo se utiliza una tarjeta de telefonía analógica y su configuración está definida en el archivo “chan_dahdi.conf”. En este archivo están configurados cuatro canales analógicos para realizar llamadas telefónicas hacia la red pública.

3.2.5.3 Configuración de los usuarios

Esta configuración permite a la aplicación servidor ASTEM conectarse con ASTERISK para realizar el monitoreo de su actividad. La configuración contenida en el archivo “manager.conf” en la carpeta de ASTERISK habilita la conexión vía TELNET para leer los eventos de la central telefónica o enviar comandos. En este archivo se encuentran también especificados los privilegios que tendrá cada usuario.

Es importante notar que se debe especificar la dirección IP para la conexión, sin embargo, en esta ocasión, se puede configurar como “localhost” o con la dirección de “loopback” 127.0.0.1 ya que el programa se ejecutará sobre el mismo servidor. También es necesario habilitar el envío de eventos CDR en el archivo “cdr_manager.conf”; esto se consigue escribiendo la línea “enable=yes”.

3.2.5.4 Configuración de CDRs

La central telefónica ASTERISK guarda un registro detallado de todas sus llamadas (CDR) en archivos separados por comas. Sin embargo, es posible configurar la central para que estos registros sean guardados en una base de datos de MySQL. Para esto se usa un complemento contenido en los “AddOns” de la PBX.

En primer lugar se crea una base de datos en MySQL con una tabla que contenga los campos de los CDR generados por ASTERISK, y un usuario con acceso a dicha tabla. Posteriormente se instalan los complementos de la PBX, y una vez

instalados se debe configurar el archivo “cdr_mysql.conf” en la carpeta de ASTERISK indicando los siguientes parámetros:

- Dirección del servidor MySQL.
- Nombre de la base de datos.
- Tabla donde se guardarán los registros CDR.
- Usuario y clave de acceso a los registros.
- Permiso de escritura en el campo “userfield”.

El permiso de escritura en el campo “userfield” permite que ASTERISK ocupe este campo con información personalizada por el usuario.

3.3 CONSIDERACIONES DE SEGURIDAD EN EL SISTEMA

La seguridad es un aspecto importante en todo desarrollo tecnológico. La tecnología de la información evoluciona a un ritmo acelerado y con ella las personas que se dedican a buscar y explotar vulnerabilidades. Por esto, hoy en día es necesario que todo desarrollo tecnológico considere, por lo menos, aspectos de seguridad mínima.

La seguridad es un tema bastante amplio del cual se podría escribir un trabajo sin profundizar demasiado. En este trabajo, se revisan dos aspectos principales de la seguridad del sistema ASTEM los cuales incluyen la seguridad en la PBX ASTERISK, y las consideraciones de seguridad en el software.

3.3.1 SEGURIDAD EN LA CENTRAL ASTERISK

La seguridad de la central ASTERISK es uno de los aspectos más delicados en este desarrollo y debe ser analizada con detenimiento a fin de evitar convertirse en víctimas de un fraude a PBX. Salvo el hecho de que utiliza TELNET para recibir conexiones de aplicaciones externas, la PBX no presenta fallas de seguridad significativas en su diseño y comúnmente los problemas de seguridad están asociados a su configuración. El punto más sensible de este tipo de centrales se encuentra en la configuración del plan de marcación y los canales.

3.3.1.1 Seguridad en los canales

Los canales de una PBX ASTERISK se configuran, según el protocolo que utilicen, en archivos de configuración donde el usuario define los parámetros de funcionamiento. Entiéndase que estos canales son los utilizados para las extensiones, es decir, cada canal le corresponderá a una extensión o a una troncal.

En el presente trabajo se utiliza protocolo SIP para dar la opción de configurar troncales que pueden ser utilizadas para conectar Gateways a la PBX. Dado que la central no manejará extensiones, no se debe configurar ningún canal adicional para usuarios. En la configuración de canales SIP se consideran los siguientes aspectos relacionados con seguridad:

- Se configuran únicamente los canales utilizados por las troncales.
- Los canales utilizados por las troncales tendrán IP estática asignada por el usuario.
- El contexto por defecto para cualquier usuario es un contexto sin ningún privilegio de llamadas.
- El contexto para los canales de las troncales es un contexto que únicamente puede recibir llamadas.
- Se configura la opción "*alwaysauthreject*" con valor "*si*" para proteger a la central frente a ataques de fuerza bruta.
- Se configura la opción "*allowguest*" con valor "*no*" a fin de evitar que usuarios anónimos se conecten al sistema.

3.3.1.2 Seguridad en el plan de marcación

El plan de marcación tendrá la configuración específica para permitir a la central realizar las pruebas de lazo cerrado únicamente. No existirá ninguna extensión adicional configurada para recibir o realizar llamadas. Adicionalmente el contexto por defecto para cualquier usuario tendrá únicamente un mensaje de advertencia para todo número que se intente marcar.

En concreto, en la configuración del plan de marcación se considerarán los siguientes aspectos relacionados con la seguridad:

- Un contexto para realizar las llamadas de lazo cerrado.
- Un contexto para recibir las llamadas de lazo cerrado.
- La configuración de las troncales.
- Contexto por defecto para limitar cualquier intento de llamada.

3.3.1.3 Seguridad física

La seguridad física suele ser poco considerada, aunque no menos importante. La ubicación de la PBX, y del sistema, será un laboratorio de la Superintendencia de Telecomunicaciones con acceso restringido únicamente a personal de la Dirección Nacional de Investigación Especial en Telecomunicaciones. De igual manera, el servidor y los equipos de telefonía se los conectará en una red diferente a la de la Superintendencia, y las claves de acceso al servidor serán conocidas únicamente por el administrador.

3.3.2 SEGURIDAD EN LA APLICACIÓN ASTEM

La aplicación distribuida ASTEM utiliza una conexión TCP por sockets para su comunicación. Esta conexión sin duda representa el reto de seguridad más relevante. Para contrarrestar un posible acceso no autorizado al sistema se adoptarán las siguientes medidas:

- El sistema autenticará únicamente a usuarios registrados en el archivo de configuración correspondiente.
- En caso de falla en la lectura de usuario, la aplicación cuenta con un usuario por defecto para ingresar. El identificador y la contraseña de este usuario serán conocidos únicamente por el administrador del programa, para ser utilizada de ser necesario.
- La autenticación de usuarios se llevará a cabo a través de un reto planteado por el servidor cuya solución deberá ser codificada.

- El servidor únicamente aceptará instrucciones de usuarios que se hayan autenticado correctamente. Caso contrario cerrará la conexión.

3.3.2.1 Proceso de autenticación de usuarios ASTEM

El sistema de autenticación de ASTEM está diseñado para proteger la contraseña del cliente durante el proceso. La contraseña no debe ser enviada durante la autenticación, en su lugar se envía un reto que el cliente debe resolver. La autenticación cuenta con 3 etapas:

1. *Solicitud*.- En esta etapa el cliente ASTEM envía una solicitud al servidor para autenticarse. El servidor como respuesta genera un reto, que consiste en un número seudo-aleatorio, y lo envía hacia el cliente. Es importante mencionar que el mensaje de autenticación es el único que el servidor acepta de una conexión nueva.

2. *Reto*.- El reto es la prueba que el cliente debe resolver. La estructura del reto y el proceso de autenticación están basados en el RFC 2617 (Autenticación HTTP), utilizado por SIP en el RFC 3261. El reto debe ser resuelto obteniendo los códigos “hash” del usuario, contraseña, y clave definida por el servidor, utilizando el algoritmo SHA-256. Posteriormente se obtiene el código “hash” de los tres códigos resultantes juntos. El resultado de este proceso constituye la solución al reto y es enviado hacia el servidor para su verificación. En la Figura 3.23 se observa un esquema del proceso de solución del reto.

3. *Verificación*.- La última etapa es el proceso de verificación. En esta etapa el servidor verifica que la respuesta enviada por el cliente corresponda con la respuesta generada localmente utilizando los datos almacenados. Si existe coincidencia el servidor envía un mensaje de bienvenida y se coloca en modo de escucha. Caso contrario envía un mensaje de error y cierra la conexión.

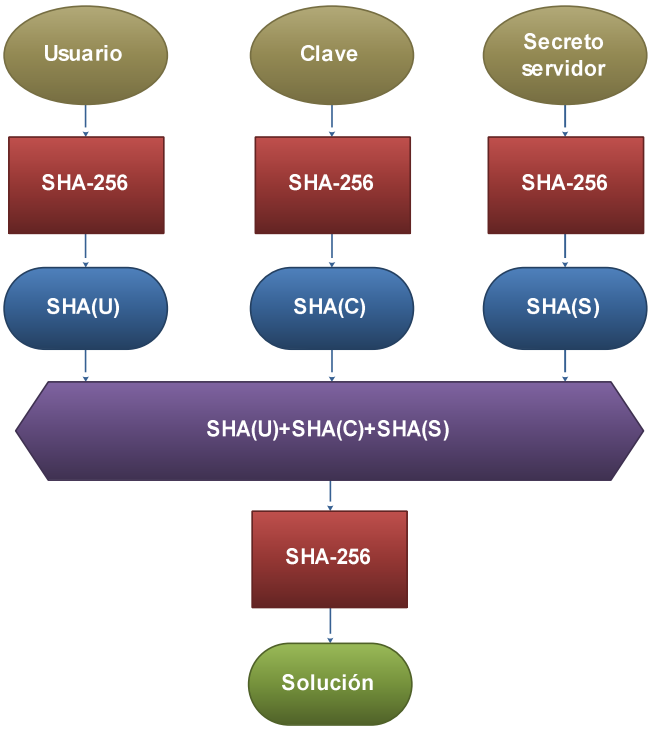


Figura 3.23. Esquema de autenticación ASTEM

3.3.3 SEGURIDAD EN EL SISTEMA OPERATIVO

En este apartado únicamente se mencionarán aspectos del sistema operativo relacionados al software ASTEM, ya que un análisis detallado de las seguridades del sistema operativo no compete al alcance de este trabajo.

El sistema operativo en el que trabajará la PBX ASTERISK y la aplicación servidor ASTEM será CentOS 5. CentOS es una distribución de Linux basada en Red Hat y orientada al manejo de servidores. El sistema operativo debe contar, al menos, con las siguientes consideraciones básicas de seguridad:

- Dirección IP privada dentro de una red independiente.
- Firewall instalado y activado.
- Puerto TCP 30003 abierto en el firewall para conexiones hacia el servidor.
- Se bloquearán en el servidor y en el enrutador los siguientes puertos:
    - Puerto 23.- Conexiones telnet por defecto.
    - Puerto 25.- Conexiones SMTP por defecto.

- Puerto 587.- Conexiones SMTP auxiliares.
- Puerto 5038.- Puerto para conexiones ASTERISK.

3.4 FORMATOS DE PRESENTACIÓN DE REPORTES

Como se ha puntualizado anteriormente, la generación automática de reportes de ASTEM permite a los usuarios extraer información de las bases de datos y guardarla en documentos con formato PDF.

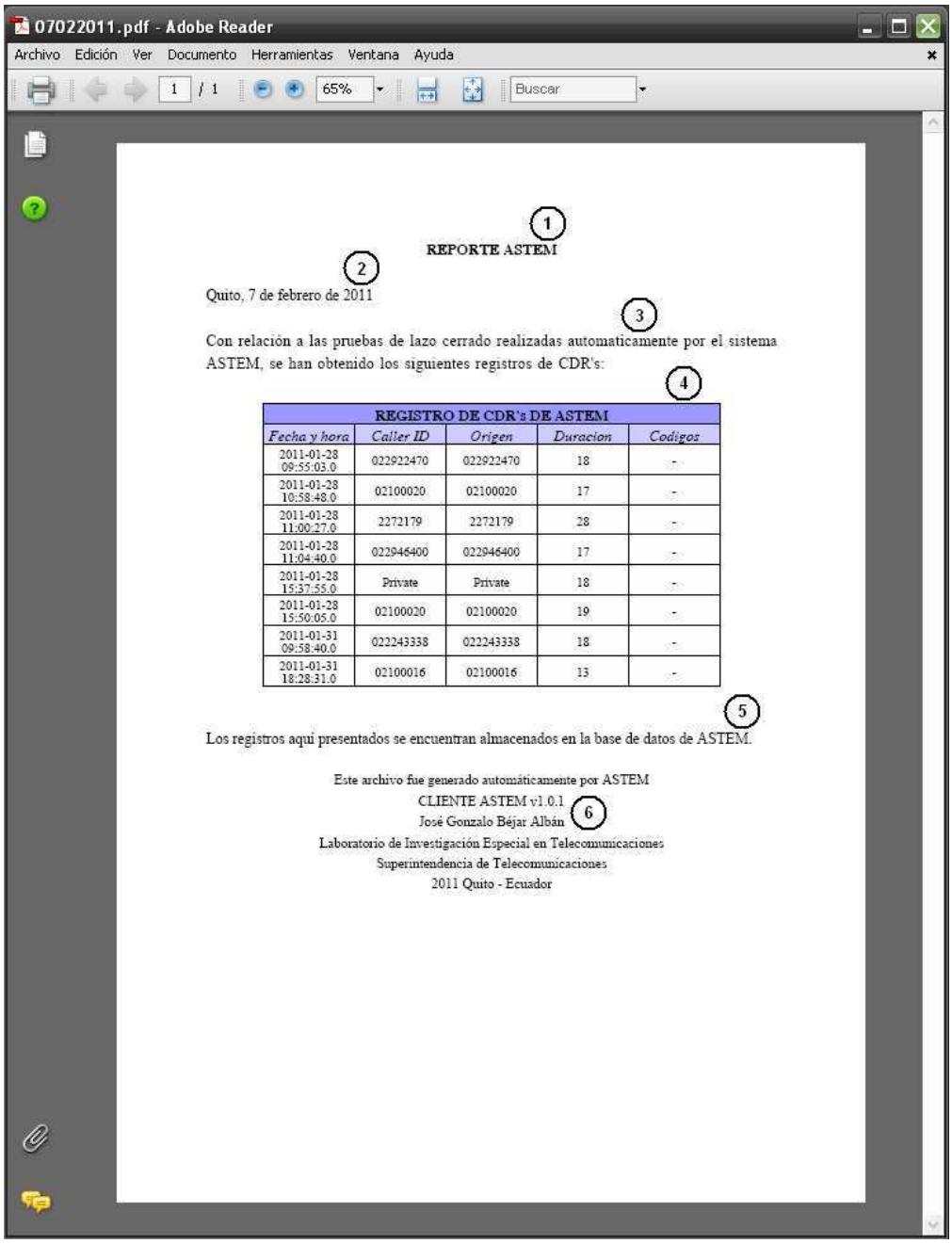


Figura 3.24. Formato de reportes generados por ASTEM

En la Figura 3.24 se puede observar un gráfico con los elementos de los informes generados por ASTEM.

1. Título.- El título del documento.
2. Fecha.- Describe la fecha en que el documento fue generado.
3. Párrafo inicial.- Contiene el texto de introducción a la información del reporte.
4. Tabla de datos.- Contiene los datos seleccionados por el usuario sobre las pruebas realizadas por el sistema y registradas en la base de datos.
5. Párrafo final.- Nota final donde se indica que la información mostrada se encuentra almacenada en la de base de datos de ASTEM.
6. Créditos.- Texto que identifica al documento como un archivo generado automáticamente por la aplicación ASTEM.

El documento PDF que crea la aplicación cliente ASTEM con la información solicitada tiene el siguiente formato:

- Tamaño de la página: A4.
- Márgenes: Definidos por el usuario (por defecto 2.5 cm en cada lado).
- Tipo de letra: Times New Roman.

3.5 IMPLEMENTACIÓN DEL SISTEMA ASTEM

El sistema ASTEM se implementará en el laboratorio de investigación especial en telecomunicaciones de la SUPERTEL, en un esquema similar al de la Figura 3.25. El desarrollo e implementación se lleva a cabo en equipos proporcionados por la SUPERTEL.

3.5.1 PARTICULARIDADES DURANTE EL DESARROLLO

Como se ha descrito anteriormente, los aspectos generales de esta solución fueron identificados y propuestos como objetivos desde el inicio. Sin embargo,

durante el desarrollo surgieron varios inconvenientes y retos que debieron ser resueltos sin alterar los planteamientos iniciales del sistema.

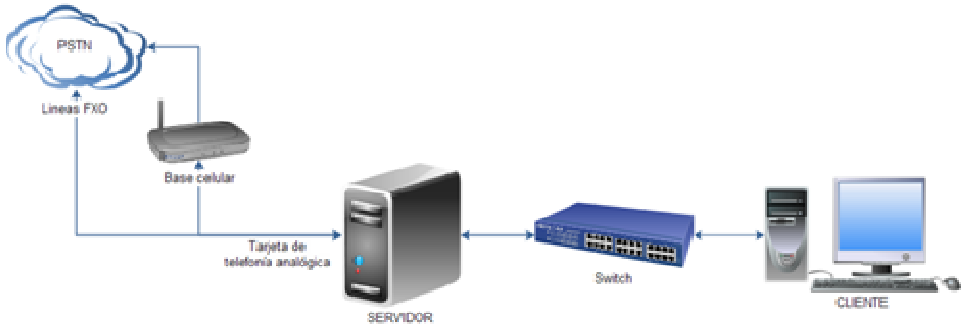


Figura 3.25. Diagrama de la implementación del sistema ASTEM

3.5.1.1 Organización de llamadas por troncales y número destino

Este problema principalmente consistió en organizar un grupo de llamadas de tal forma que le corresponda un número destino a una sola troncal. Los números destino no se deben repetir ya que esto podría acarrear pruebas fallidas. Para esto se estructuró un método que de forma individual determina que números le corresponden a cada troncal y los asigna de forma que no puedan tener dos troncales un mismo número destino.

3.5.1.2 Generación de llamadas por grupos

Lo más sencillo para generar un grupo de llamadas en una PBX ASTERISK sería colocar todos los archivos en la carpeta correspondiente. Sin embargo, esto hace que ASTERISK intente generar todas las llamadas al mismo momento provocando que las troncales se saturen. En consecuencia, la mayoría de llamadas no se podrá completar ya que las líneas estarán ocupadas.

Para esto se debe determinar cuántas llamadas simultáneas se deben generar y que troncales lo harán, ya que una troncal genera una sola llamada. Este problema se solucionó utilizando carpetas para dividir las llamadas en grupos. Primero la central identifica cuantas llamadas simultáneas puede realizar con las troncales indicadas, y asigna grupos con esa cantidad de llamadas. Luego cada cierto tiempo (configurable en el sistema) copia un grupo de llamadas en la central para que sean procesadas. El tiempo de espera estará definido por la duración máxima de una llamada de prueba.

3.5.1.3 Envío de la configuración a través de la conexión

A fin de evitar transmitir información de configuración redundante, la configuración del sistema es codificada de forma que cada grupo y cada campo del grupo es reemplazado por un número que lo identifica en el lado del cliente; y, para enviar la configuración se utiliza el formato “grupo:campo:valor”. Por ejemplo, el campo “clave” del grupo “monitor” tiene un valor “contraseña”; el grupo “monitor” es identificado por el número 3, y el campo “clave” por el número 4, por lo cual esta información se codificará como “3:4:contraseña” para ser enviada al cliente.

3.5.1.4 Envío de los datos de una consulta a la base de datos

El principal problema en este proceso es el envío de grandes cantidades de información. Por ejemplo, una consulta a la base de datos puede devolver tal cantidad de información que ésta no podría ser enviada en un solo mensaje, y sería necesario dividirla en partes. Aprovechando que se utiliza con una conexión TCP, esto se resolvió enviando cada fila de una consulta como un mensaje independiente. Cada mensaje contiene una bandera al final que indica al cliente si el mensaje es el último o si debe esperar más mensajes. Adicionalmente, en el lado del cliente, se puede seleccionar campos específicos para una consulta y definir filtros a fin de disminuir la cantidad de información transmitida.

Otro reto dentro de este problema fue definir desde donde se debían realizar las consultas a la base de datos, desde el lado del cliente o del servidor. Se optó por realizar las consultas desde el servidor para que únicamente éste tenga acceso a la base de datos, lo cual además implica mayor seguridad.

3.5.1.5 Generación de reportes

Este problema radicó en la implementación de un módulo que permita generar archivos PDF en base a datos contenidos en una tabla. Este problema se solucionó de forma rápida utilizando un API iText de JAVA.

3.5.1.6 Manejo de hilos en ASTEM

Durante el desarrollo del sistema surgieron dificultades en la sincronización de hilos paralelos que acceden a métodos comunes y el paso de mensajes entre

dichos hilos. Estos inconvenientes se solucionaron utilizando API's de JAVA para el manejo de hilos, e interfaces para el intercambio de mensajes.

3.5.2 CONSOLA DE USUARIO DEL SERVIDOR ASTEM

La aplicación servidor ASTEM interactúa con un usuario en el equipo a través de una consola. A través de la consola, el programa recibe comandos para ejecutar instrucciones específicas. Véase la Figura 3.26.

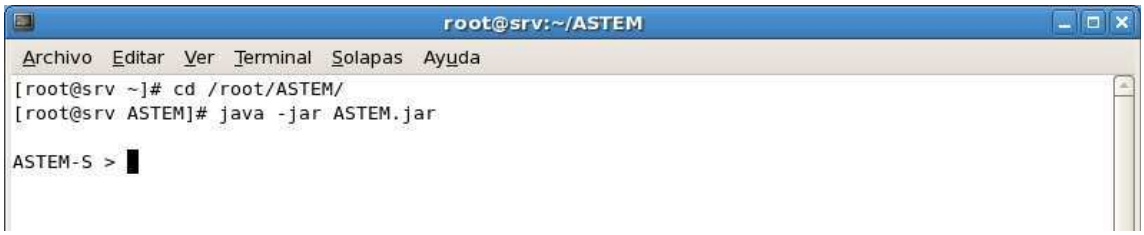


Figura 3.26. Consola de la aplicación servidor ASTEM

Algunas instrucciones que el programa interpreta pueden ser introducidas únicamente por consola, y otras a través de una conexión de red. A continuación se presenta la lista de instrucciones que el programa recibe por consola y sus opciones.

3.5.2.1 Instrucción 'llamar'

La instrucción "llamar" origina una llamada o un grupo de llamadas a un mismo destino utilizando una sola tarjeta de telefonía. Se debe especificar el teléfono de origen, destino, tarjeta y número de llamadas. Este comando no se utiliza para generar grupo de llamadas, únicamente para generar una llamada a la vez.

Sintaxis: llamar [tarjeta] [teléfono] [troncal] [repeticiones]

Opciones:

- *tarjeta*.- Contiene el código de la tarjeta que se desea utilizar.
- *teléfono*.- Contiene el ID del teléfono destino.
- *troncal*.- Contiene el ID de la troncal que generará la llamada.
- *repeticiones*.- Define el número de veces que se realizará la llamada.

3.5.2.2 Instrucción ‘tarjeta’

Utilizando la instrucción “tarjeta” se puede realizar la administración de la base de datos de tarjetas guardadas en el sistema. Junto al comando “tarjeta” se debe especificar la acción a realizar que puede ser actualizar, guardar, o borrar, y los datos necesarios para ejecutar la instrucción.

Otra forma de modificar la configuración de las tarjetas es a través del archivo “tarjeta.astem”. El archivo contiene los datos de las tarjetas, sin embargo, para aplicar cualquier cambio efectuado directamente sobre los archivos es necesario reiniciar la aplicación.

Sintaxis: tarjeta actualizar/borrar/guardar [datos]/[ID]/!

Opciones:

- *actualizar*.- Ejecuta el comando de actualización de datos de una tarjeta, o agrega una tarjeta nueva. Esta opción va seguida de los datos de la tarjeta. Los datos deben ir en el siguiente orden y separados por comas: ID, nombre, código de país, número de acceso, opción de idioma, tiempo de idioma, número de pin, tiempo de pin y código internacional.

- *borrar*.- Elimina una tarjeta de los registros del programa. Para ejecutar este comando es necesario especificar el ID de la tarjeta a eliminar.

- *guardar*.- Este comando almacena los datos de las tarjetas reescribiendo el archivo “tarjeta.astem” con los datos que tenga el programa en ese momento. Este comando es necesario para guardar de forma permanente cualquier cambio que se haya realizado.

3.5.2.3 Instrucción ‘consulta’

La instrucción consulta solicita al sistema la ejecución de sentencias MySQL de consulta sobre la base de datos del sistema. Este comando es utilizado tanto para consultas de CDR’s como de notificaciones, y admite parámetros para filtrar la información solicitada.

Sintaxis: consulta <cdr/notificacion> [campos] [condición]

Opciones:

- *cdr*.- Ejecuta la instrucción de consulta sobre la base de datos de CDR's almacenados por la PBX ASTERISK.
- *notificacion*.- Ejecuta la instrucción de consulta sobre la base de datos de notificaciones almacenadas por el sistema.
- *campos*.- Contiene los campos que se desee consultar en la base de datos. Si esta opción se la deja en blanco, se consultan todos los campos.
- *condición.*- Contiene la condición de consulta. La condición debe tener el formato de una condición MySQL, Si la condición se mantiene en blanco, la consulta se realiza sin condiciones.

3.5.2.4 Instrucción 'astem'

La instrucción "astem" maneja las opciones de configuración del sistema ASTEM y de los usuarios. A través de las opciones de esta instrucción, se puede consultar la configuración del sistema, modificarla o guardarla.

Otra forma de modificar la configuración es a través de los archivos de configuración. Sin embargo, al igual que en la administración de tarjetas, es necesario parar e iniciar la aplicación nuevamente para aplicar los cambios. Más adelante se detalla la estructura de los archivos de configuración.

Sintaxis: astem consulta/configurar/guardar configuracion/usuarios/llamar/tarjeta actualizar/eliminar/[campos] [campos]

Opciones:

- *consulta*.- Solicita información a la aplicación servidor sobre una característica en particular. Las solicitudes pueden ser:
    - *configuracion*.- Solicita la configuración actual del sistema.
    - *usuarios*.- Solicita la lista de usuarios y contraseñas.
    - *llamar*.- Solicita los datos de tarjetas, troncales y números.

- *tarjeta*.- Solicita los datos de las tarjetas contenidas en el sistema.

- *configurar*.- Permite cambiar parámetros en la configuración del sistema. Las opciones que esta instrucción admite son las siguientes:

  - *configuracion*.- Modifica opciones de la configuración del servidor.

  - *usuarios*.- Agrega, actualiza o elimina un usuario del sistema.

  Una vez especificada la opción a actualizar, se ingresan la información codificada.

- *guardar*.- Almacena los datos de configuración de forma permanente reescribiendo los archivos “admin.astem” y “usuarios.astem”. Esta opción debe tener como parámetro final el comando “!”.

3.5.2.5 Instrucción ‘asterisk’

La instrucción “asterisk” está implementada para administrar la configuración de la PBX ASTERISK leyendo y sobrescribiendo sus archivos. Este comando permite únicamente los parámetros necesarios en los archivos de configuración de la PBX. Si se desea modificar parámetros adicionales es necesario hacerlo directamente en los archivos, sin alterar la estructura definida por el sistema.

Sintaxis: asterisk <general/sip/eliminar/aplicar/consulta> [datos]

Opciones:

- *general*.- Realiza una actualización sobre la configuración del plan de marcación, el archivo de conexiones remotas y los datos de la base de datos utilizada por la PBX para guardar los CDR’s generados.

- *sip*.- Realiza la actualización de las opciones de los canales SIP, y las troncales configuradas en la PBX.

- *eliminar*.- Permite eliminar una troncal SIP de la configuración de la PBX.

- *aplicar*.- Guarda los cambios realizados en los archivos de configuración de la PBX sobrescribiendo sus archivos, y ejecuta el comando de reinicio de la misma para que la nueva configuración sea aplicada.

- *consulta*.- Solicita información a la aplicación servidor de la configuración actual de la PBX ASTERISK. El sistema responde luego de leer los archivos de la PBX y codificar los datos.

3.5.2.6 Instrucción 'cronograma'

La instrucción "cronograma" realiza una función similar a la instrucción "llamar", con la diferencia de que ejecuta un grupo de llamadas utilizando una lista de troncales, números destino y tarjetas.

Al ejecutar el comando, el sistema organiza automáticamente los archivos en grupos de llamadas para que sean colocadas en la PBX en el orden adecuado, asegurando que se realiza el número de prueba posible con la lista de troncales y destinos especificados. En otras palabras, el sistema asigna al menos un número telefónico destino a cada troncal, y una sola troncal a un número telefónico destino. Esto con el fin de tener una única llamada originada a ese número destino al mismo tiempo. Cumplir con esta condición es necesario para ejecutar las llamadas simultáneas sin que se crucen entre sí.

La instrucción tiene también la opción de ejecutar inmediatamente las llamadas de pruebas especificadas, o programar una fecha y hora para que se lleven a cabo. Cualquiera que sea el caso, debe ser especificado en la instrucción.

Sintaxis: cronograma ejecutar/[fecha hora] [troncales] [tarjetas] [destinos-cantidad] [intentos]

Opciones:

- *ejecutar*.- Esta opción ejecuta las pruebas de lazo cerrado de forma inmediata, una vez los grupos hayan sido construidos.

- *fecha y hora*.- Reemplaza la opción “ejecutar” y especifica la fecha y hora en que las pruebas deben ser ejecutadas. El formato que el sistema reconoce es: dd/MM/yyyy HH:mm:ss.

- *troncales*.- Contiene las ID’s de las troncales que se utilizarán para generar las llamadas. Los ID’s van separados por comas.

- *tarjetas*.- Contiene los códigos de las tarjetas que se desea utilizar en las llamadas de prueba. Los códigos van separados por comas.

- *destinos-cantidad*.- Contiene los códigos de los números destino y el número de llamadas que se deben realizar a cada destino. Las códigos a utilizar van separados por comas, y la cantidad de llamadas se escribe junto al código, separado por un “/”. Por ejemplo, para especificar 5 llamadas al número con código 1 se escribe “1/5”.

- *intentos*.- Un número que define la cantidad de intentos que la PBX debe realizar si una llamada es contestada por la operadora.

3.5.2.7 Instrucción ‘estado’

La instrucción “estado” tiene dos funciones. La primera es consultar el estado del hilo monitor del sistema y las llamadas que se encuentran pendientes por realizar. La segunda es activar o desactivar el hilo que monitorea la actividad de la PBX. Es importante mencionar que en caso de que el monitor se encuentre desactivado, el sistema lo activa automáticamente el momento de iniciar una prueba de lazo cerrado.

Sintaxis: estado <consulta/monitor/borrar> <si/no>

Opciones:

- *consulta*.- Ejecuta una consulta sobre el estado del servidor.

- *borrar*.- Elimina las pruebas de lazo cerrado pendientes. Esto no incluye las pruebas que se encuentran programadas y no han sido ejecutadas aún.

- *monitor*.- Activa o desactiva el hilo del sistema que monitorea las llamadas. Para activarlo se utiliza el parámetro “si”, caso contrario el parámetro “no”.

3.5.2.8 Instrucción ‘debug’

La instrucción “debug” activa o desactiva la publicación de mensajes en consola. Los mensajes que son guardados en los archivos de registro de ASTEM se muestran en consola si la opción se encuentra activa.

Sintaxis: debug [on/off]

Opciones:

- *on*.- Activa la publicación de mensajes del sistema en consola.
- *off*.- Desactiva la publicación de mensajes del sistema en consola.

3.5.2.9 Instrucción ‘quit’

El comando “quit” finaliza la aplicación cerrando todos los procesos que se encuentra ejecutando. Esta instrucción únicamente tiene la opción de fin “!”.

Sintaxis: quit !

3.5.2.10 Archivos de configuración del sistema

El sistema ASTEM maneja principalmente 4 archivos en el lado del servidor, de los cuales 3 están destinados para opciones de configuración y 1 para el registro de actividad. Es necesario detallar la estructura de los archivos de configuración en caso de que el usuario desee modificarlos manualmente. En todos los archivos se reconoce el símbolo “;” como carácter especial que determina el inicio de comentarios, por lo cual cualquier texto introducido después no es leído. Los archivos de configuración son:

- admin.astem
- usuarios.astem
- tarjeta.astem

3.5.2.10.1 Estructura del archivo admin.astem

El archivo “admin.astem” contiene las principales configuraciones de la aplicación servidor. Este archivo se encuentra estructurado por grupos, donde cada grupo se identifica utilizando una etiqueta, y todos los parámetros contenidos debajo de la etiqueta pertenecen al grupo. La etiqueta se escribe utilizando corchetes.

Los parámetros de configuración de un grupo terminan el momento en que otra etiqueta define un nuevo grupo. En adelante, los parámetros identificados serán asignados al grupo definido. Los grupos y parámetros de configuración son los descritos en la Tabla 3.20.

Grupo	Parámetros
astem	puerto cola
operadora	intentos espera tiempo_grupos codigo_internacional codigo_pais
monitor	host puerto usuario clave
mysql	host base tabla_cdr tabla_notificacion usuario clave
alertas	mail
servidor_mail	host ttls puerto_smtp

Grupo	Parámetros
servidor_mail_aux	usuario
	autenticacion
	cuenta
	clave
	host
	ttls
	puerto_smtp
	usuario
	autenticacion
	cuenta
	clave
troncales	troncal1
	troncal2
	…
numeros	numero1
	numero2
	…

Tabla 3.20. Opciones de configuración del archivo “admin.astem”.

3.5.2.10.2 Estructura del archivo usuarios.astem

El archivo “usuarios.astem” mantiene una estructura simple, donde el nombre de usuario se especifica entre corchetes. A continuación, la contraseña se especifica utilizando el parámetro “clave”.

[usuario]

clave=contraseña

3.5.2.10.3 Estructura del archivo tarjeta.astem

La estructura del archivo “tarjeta.astem” es bastante sencilla. Este archivo únicamente contiene la información de las tarjetas prepago. Cada tarjeta se escribe en una línea diferente, con sus datos separados por comas. La estructura es la siguiente:

…

CÓDIGO, nombre, número de salida internacional, número de acceso, opción de idioma, tiempo de idioma, número PIN, tiempo de PIN, código de discado internacional, tiempo de espera para marcar el teléfono destino

…

CAPÍTULO 4

PRUEBAS DEL SISTEMA, BENEFICIOS Y LIMITACIONES

4.1 PRUEBAS REALIZADAS

Para comprobar el correcto funcionamiento de todas las funciones del sistema se plantean 12 escenarios en los cuales se utilizará un servidor con una tarjeta analógica de 4 puertos FXO para conectar las líneas telefónicas. Cada escenario tiene como fin comprobar el funcionamiento de un aspecto en particular del sistema. Las pruebas realizadas son:

1. Conexión entre la aplicación cliente y servidor.
2. Administración de tarjetas de telefonía pre-pagada.
3. Modificar las configuraciones del sistema ASTEM.
4. Modificar las configuraciones de la PBX ASTERISK.

5. Generar llamadas de prueba a un número de destino.
6. Programar un grupo de llamadas de prueba.
7. Identificar el campo de *Caller ID* en una llamada de lazo cerrado
8. Identificación de alertas y envío de notificaciones.
9. Realizar una consulta a los CDR de ASTEM.
10. Realizar una consulta a los CDR de ASTERISK.
11. Datos estadísticos del sistema.
12. Registros del sistema ASTEM.

Figura 4.1. Ventana de información del sistema

4.1.1 CONEXIÓN ENTRE LA APLICACIÓN CLIENTE Y SERVIDOR

Propósito:

- Establecer la conexión entre la aplicación cliente y servidor.

- Comprobar el funcionamiento del módulo de autenticación.
- Comprobar el acceso a las diferentes funciones del programa.
- Realizar el proceso de desconexión de la aplicación cliente.

Contexto:

La aplicación servidor ASTEM es instalada en un servidor con sistema operativo CentOS 5.4 y una tarjeta de telefonía analógica de 4 puertos FXO; y se encuentra configurada para que escuche conexiones TCP en el puerto 30003. En el mismo servidor se encuentra instalada la PBX ASTERISK. El equipo se encuentra conectado a una red LAN en la red 192.168.1.0 a través de un *switch*. En la misma red se encuentra conectado un computador con sistema operativo Windows XP, el cual será utilizado para ejecutar la aplicación cliente y realizar la conexión con el servidor.

Procedimiento:

1. Configurar el servidor con la IP 192.168.1.254/24.

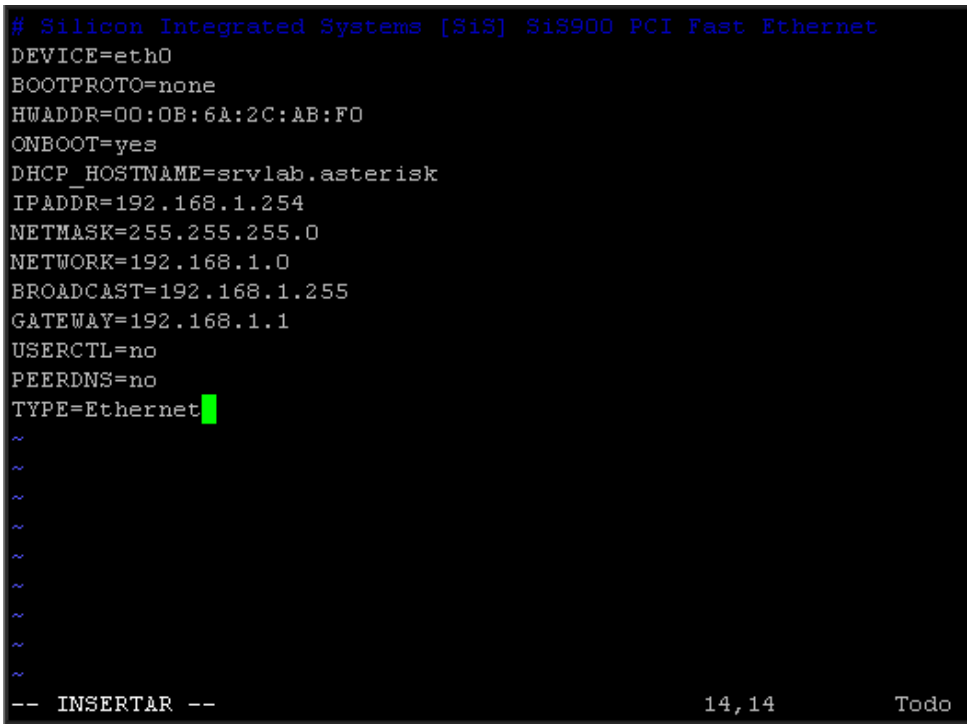


Figura 4.2. Archivo de configuración de red del equipo servidor

2. Iniciar la aplicación servidor ASTEM.

3. Configurar el computador con Windows XP con una IP de la red 192.168.1.0/24.

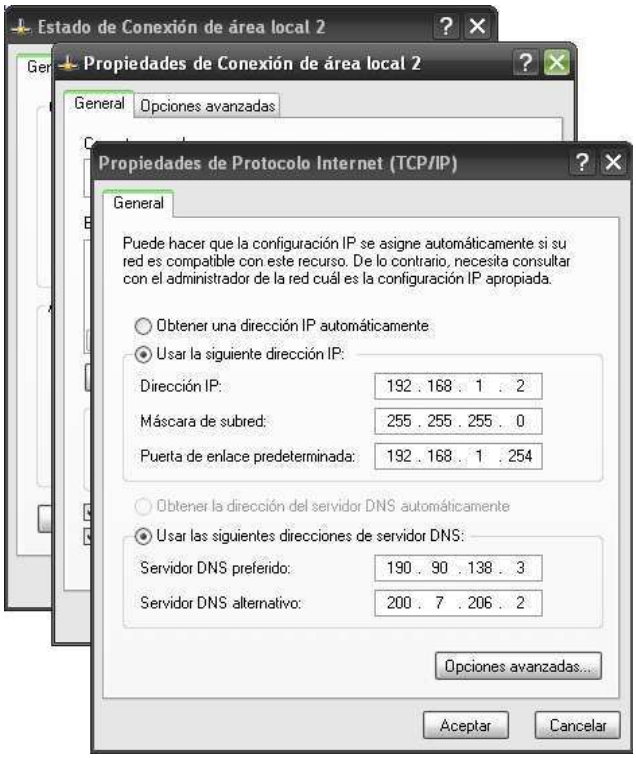


Figura 4.3. Configuración de los parámetros de red en el equipo cliente

4. Iniciar la aplicación cliente ASTEM.
5. Seleccionar la opción “Conectar” en el cliente.
6. Ingresar los siguientes datos de usuario incorrectos:
    a. Usuario: nombre
    b. Clave: secreto

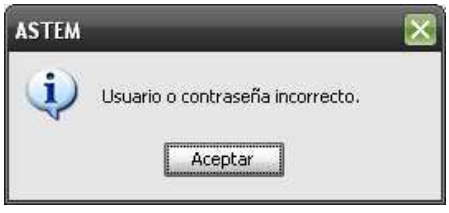


Figura 4.4. Mensaje de respuesta del servidor cuando la autenticación falla

7. Verificar la respuesta del servidor.
8. Ingresar los siguientes datos de usuario correctos:

a. Usuario: jgomez

b. Clave: *12345*

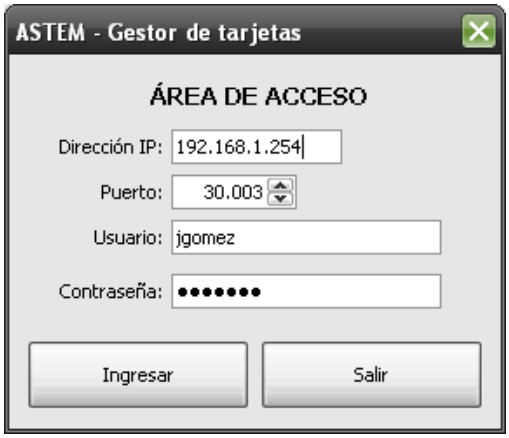


Figura 4.5. Ventana de autenticación de la aplicación cliente

9. Verificar la respuesta del servidor y acceso a las opciones del programa.

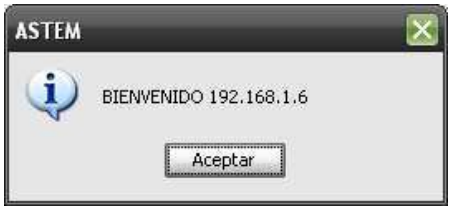


Figura 4.6. Mensaje de autenticación confirmada

10. Comprobar el acceso a todas las ventanas del menú principal.

Figura 4.7. Ventana principal del sistema ASTEM

11. En el menú principal, seleccionar la opción desconectar.

Figura 4.8. Opción “Desconectar” en la ventana principal del sistema

12. Verificar el mensaje de respuesta y el bloqueo de las opciones del programa.

13. Salir de la aplicación.

Figura 4.9. Mensaje de finalización de la conexión con el servidor

Resultados:

- La conexión fue exitosa. Se consiguió acceso a todas las opciones del programa utilizando un nombre de usuario y clave correctos.
- El programa no aceptó la conexión al utilizar un nombre de usuario o clave incorrectos. Las opciones se mantuvieron bloqueadas.

Observaciones:

- El tiempo de conexión depende de la velocidad de la red. En una red congestionada puede tardar unos segundos hasta realizarse.

4.1.2 ADMINISTRACIÓN DE TARJETAS DE TELEFONÍA PRE-PAGADA

Propósito:

- Recibir los datos de las tarjetas almacenadas en el sistema.

- Modificar los valores de configuración de las tarjetas almacenadas.
- Agregar una tarjeta al registro.
- Eliminar una tarjeta del registro.
- Guardar los cambios realizados en el archivo de registro de tarjetas.

Contexto:

Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente. En el servidor se encuentran registradas 3 tarjetas de telefonía pre-pagada, en las cuales se realizarán las pruebas de configuración.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de administración de tarjetas.

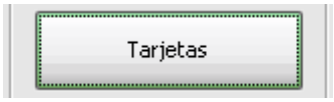


Figura 4.10. Botón de la ventana de administración de tarjetas

3. Navegar entre las tarjetas almacenadas en el sistema.

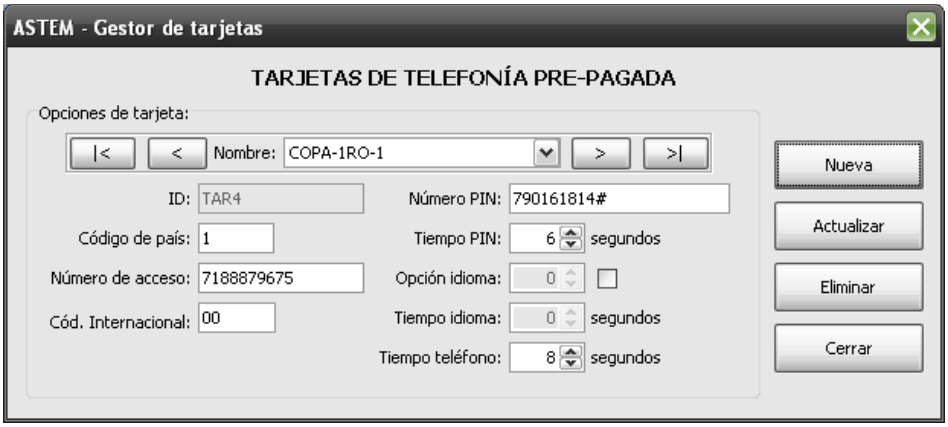


Figura 4.11. Ventana del administrador de tarjetas del sistema

4. Modificar y guardar los datos de la tarjeta TAR4 con los siguientes valores:
    a. Nombre: COPA-1RO-1

b. Tiempo de PIN: 4

c. PIN: 7901618145#

d. Código de país: 1

e. Número de acceso: 7188879670

f. Código de salida internacional: 00

g. Tiempo de idioma: Activado

h. Opción de idioma: 2

i. Tiempo teléfono: 6

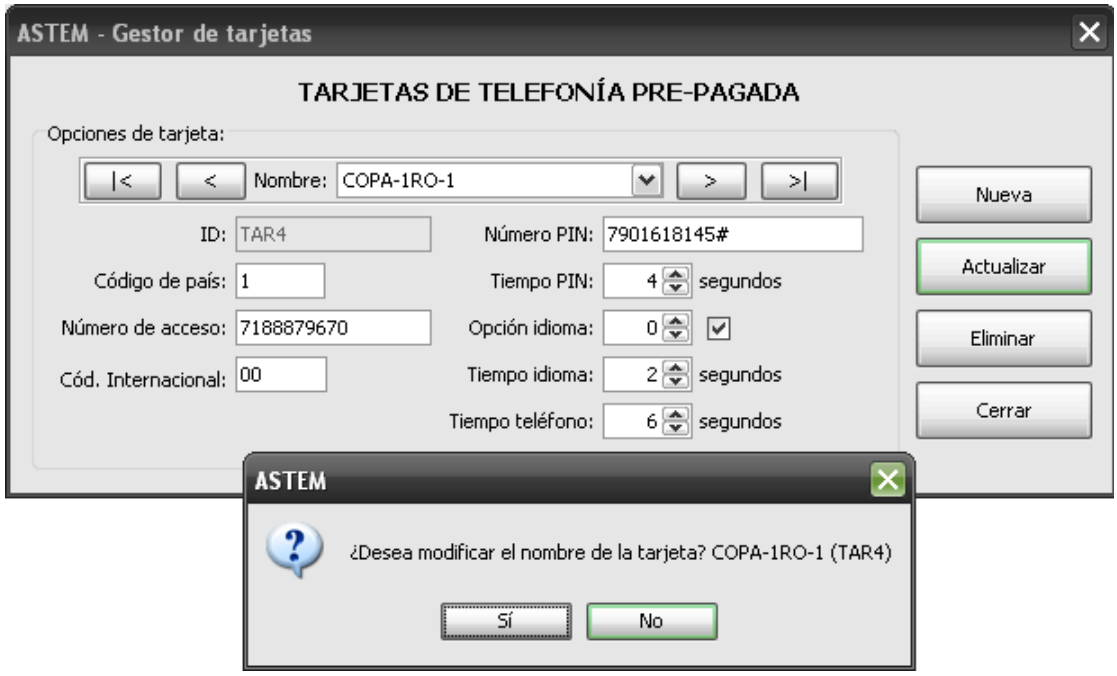


Figura 4.12. Mensaje de actualización de los datos de la tarjeta

5. Verificar que los datos han sido guardados.

6. Seleccionar la opción “Nueva” y agregar una nueva tarjeta de telefonía con los siguientes datos:

   a. Nombre: SIBRAVO-QE-6

   b. Tiempo de PIN: 4

c. PIN: 7080189391#

d. Código de país: 1

e. Número de acceso: 7185771684

f. Código de salida internacional: 00

g. Tiempo de idioma: Desactivado

h. Opción de idioma: N/A

i. Tiempo teléfono: 6

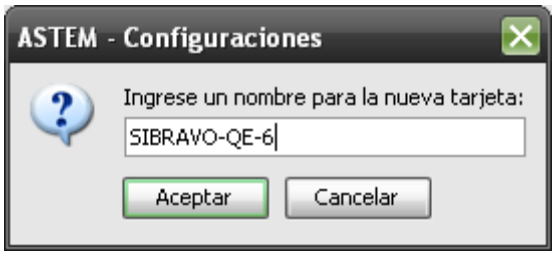


Figura 4.13. Primer mensaje de ingreso de una nueva tarjeta

7. Verificar que la nueva tarjeta ha sido agregada al registro.

8. Seleccionar la opción “Eliminar” para eliminar el registro de la tarjeta agregada.

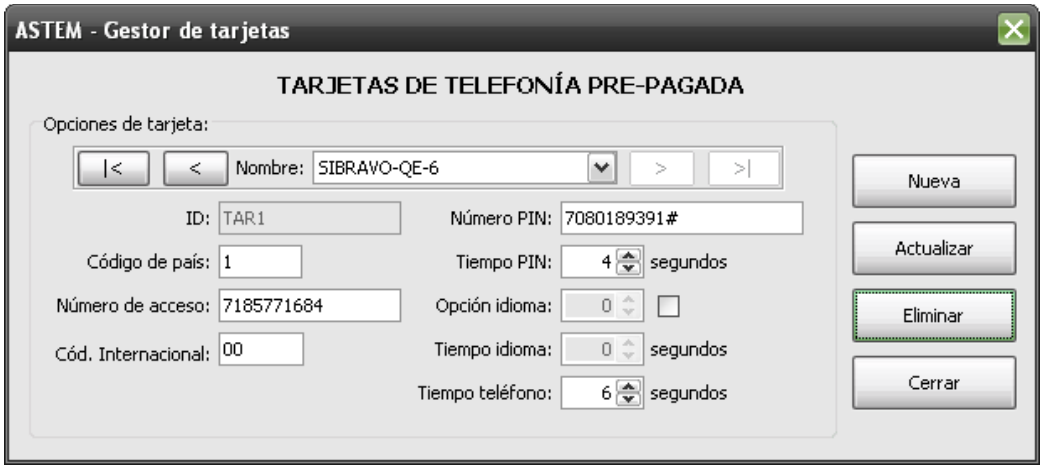


Figura 4.14. Opciones de la tarjeta eliminada

9. Comprobar que la tarjeta ha sido eliminada de los registros.

Figura 4.15. Mensaje de confirmación de que la tarjeta ha sido borrada

10. Cerrar la ventana de administración de tarjetas. Aparecerá un cuadro donde se pregunta si se desea guardar los cambios de forma permanente.

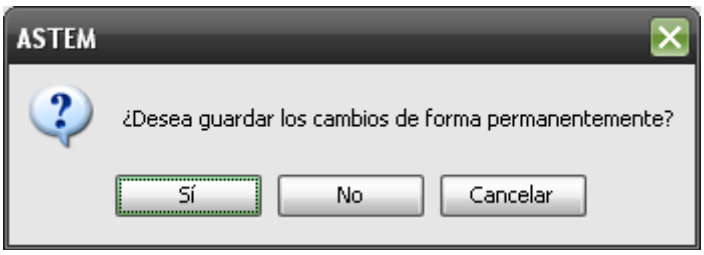


Figura 4.16. Mensaje de cierre de la ventana de configuraciones del sistema

11. Comprobar que el archivo de tarjetas fue actualizado.

Resultados:

- El registro de tarjetas pudo ser modificado y actualizado con éxito. Utilizando el menú para administración de tarjetas se pudo actualizar los datos de una tarjeta almacenada, agregar tarjetas adicionales, y eliminar una tarjeta.

Observaciones:

- Es posible agregar una tarjeta utilizando datos de una tarjeta ya almacenada anteriormente. Esta opción es útil al añadir tarjetas del mismo proveedor sin necesidad de llenar nuevamente todos los campos.
- Al agregar una nueva tarjeta todas las demás opciones del administrador quedan bloqueadas. Una vez que se guarde la nueva tarjeta, o se cancele, las opciones vuelven a estar disponibles.

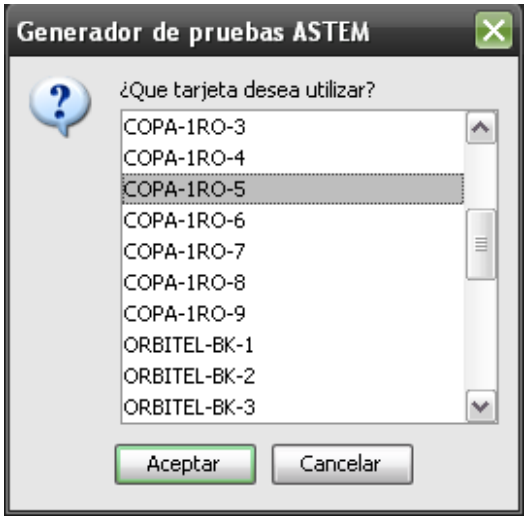


Figura 4.17. Ventana de selección de una tarjeta modelo

4.1.3 MODIFICAR LAS CONFIGURACIONES DEL SISTEMA ASTEM

Propósito:

- Visualizar la configuración de la aplicación servidor ASTEM.
- Modificar las configuraciones en la aplicación servidor ASTEM.
- Modificar la configuración de usuarios del sistema ASTEM.
- Guardar la configuración en los archivos de ASTEM.

Contexto:

Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente. El servidor se encuentra utilizando las configuraciones por defecto, la cual será modificada.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de configuración de ASTEM a través de la opción “Configuración”.

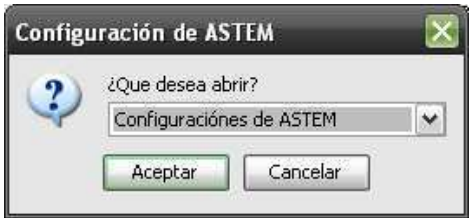


Figura 4.18. Ventana de ingreso a la configuración ASTEM

3. Visualizar la configuración del sistema ASTEM.

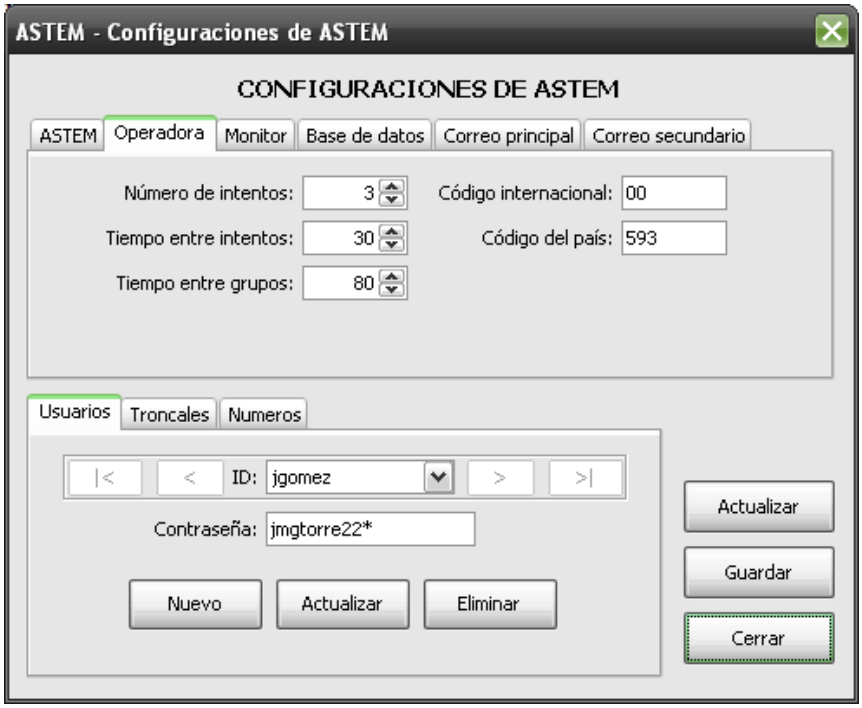


Figura 4.19. Ventana de configuraciones del sistema

4. Realizar cambios en las configuraciones de la pestaña ASTEM.

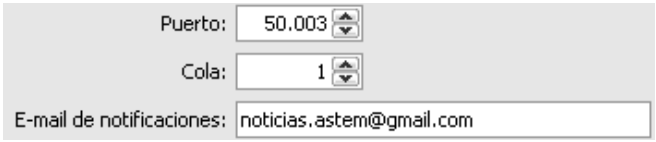


Figura 4.20. Opciones modificadas en la pestaña ASTEM

5. Verificar que los datos hayan sido actualizados.

6. Realizar cambios en las configuraciones de la pestaña Operadora.

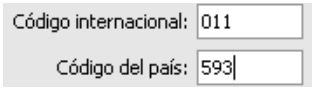


Figura 4.21. Opciones modificadas en la pestaña Operadora

7. Verificar que los datos hayan sido actualizados.

8. Realizar cambios en las configuraciones de la pestaña Monitor.

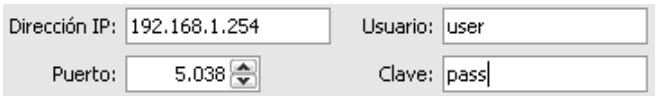


Figura 4.22. Opciones modificadas en la pestaña Monitor

9. Verificar que los datos hayan sido actualizados.

10. Realizar cambios en las configuraciones de la pestaña Base de datos.

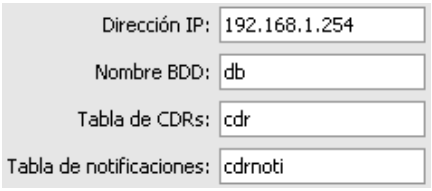


Figura 4.23. Opciones modificadas en la pestaña Base de datos

11. Verificar que los datos hayan sido actualizados.

12. Realizar cambios en las configuraciones de la pestaña Correo principal.

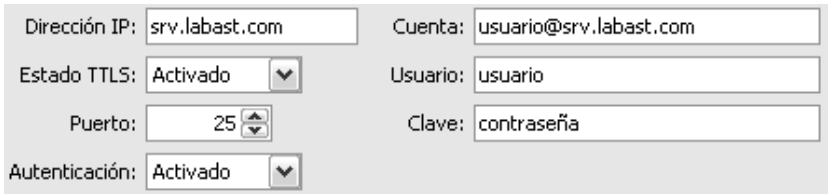


Figura 4.24. Opciones modificadas en la pestaña Correo principal

13. Verificar que los datos hayan sido actualizados.

14. Realizar cambios en las configuraciones de la pestaña Correo secundario.

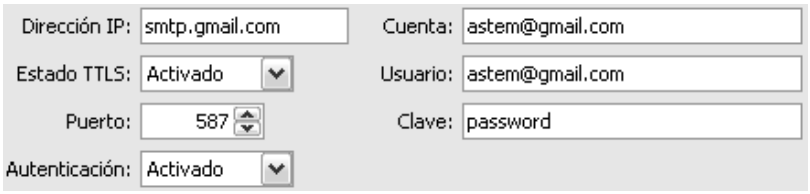


Figura 4.25. Opciones modificadas en la pestaña Correo secundario

15. Verificar que los datos hayan sido actualizados.

16. Realizar cambios en las configuraciones de la pestaña Usuario.

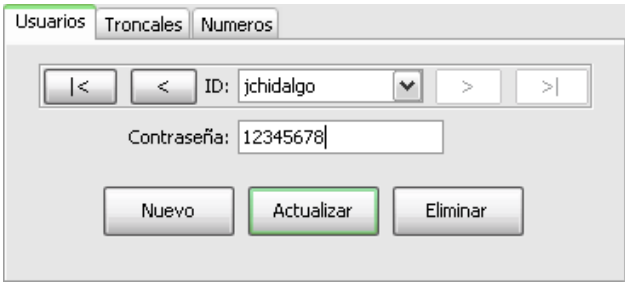


Figura 4.26. Opciones modificadas en la pestaña Usuario

17. Verificar que los datos hayan sido actualizados.

18. Realizar cambios en las configuraciones de la pestaña Troncales.

Figura 4.27. Opciones modificadas en la pestaña Troncales

19. Verificar que los datos hayan sido actualizados.

20. Realizar cambios en las configuraciones de la pestaña Números.

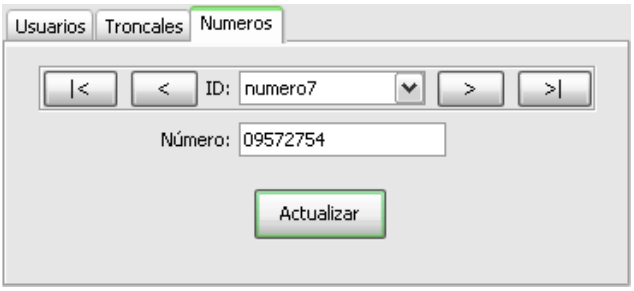


Figura 4.28. Opciones modificadas en la pestaña Números

21. Verificar que los datos hayan sido actualizados.

22. Guardar la configuración en los archivos de ASTEM.

Figura 4.29. Botones de la ventana de configuración del sistema

23. Cerrar la ventana de configuración de la aplicación.

24. Comprobar que el archivo de configuración de ASTEM fue actualizado.

Resultados:

- La configuración almacenada en el sistema pudo ser modificada utilizando la ventana de administración. Los cambios realizados se guardaron con éxito en el archivo de configuración y las diferentes opciones permitieron actualizar todos los campos en el sistema.
- Los datos de usuarios, troncales y números fueron actualizados correctamente.

Observaciones:

- El botón actualizar sobre el botón guardar aplica únicamente para las opciones superiores que se encuentran visibles; es decir, este botón no guarda los datos de usuarios troncales o números. Para almacenar cambios en la configuración de usuarios, troncales o números se debe utilizar los botones propios de cada recuadro.
- La opción guardar aplica todos los cambios en los archivos de configuración. Si se cierra la ventana sin actualizar la configuración se pierde esta información

4.1.4 MODIFICAR LAS CONFIGURACIONES DE LA PBX ASTERISK

Propósito:

- Visualizar los aspectos más relevantes de la configuración de la PBX utilizando la aplicación cliente ASTEM.
- Modificar aspectos de la configuración de la PBX ASTERISK utilizando la aplicación cliente ASTEM.
- Aplicar los cambios realizados a la configuración de la PBX ASTERISK utilizando la aplicación cliente ASTEM.

Contexto:

En el servidor, la PBX ASTERISK se encuentra configurada de acuerdo a la estructura del sistema y funcionando correctamente. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de configuraciones de ASTERISK a través de la opción “Configuración”.

Figura 4.30. Ventana de ingreso a la configuración ASTERISK

3. Visualizar la configuración de la PBX ASTERISK.
4. Realizar cambios en las configuraciones de la pestaña Plan de Marcación.

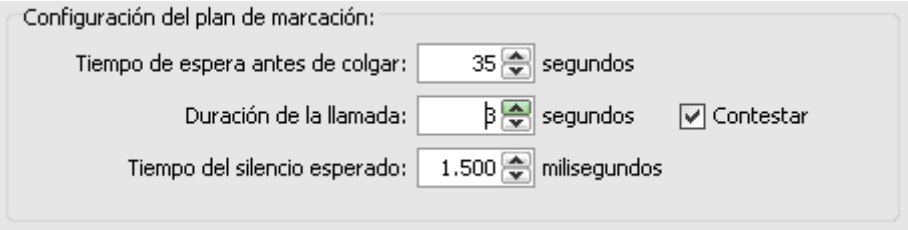


Figura 4.31. Opciones modificadas en la pestaña Plan de marcación

5. Verificar que los datos hayan sido actualizados y realizar modificaciones de otros parámetros.
6. Realizar cambios en las configuraciones de la pestaña Canales SIP.

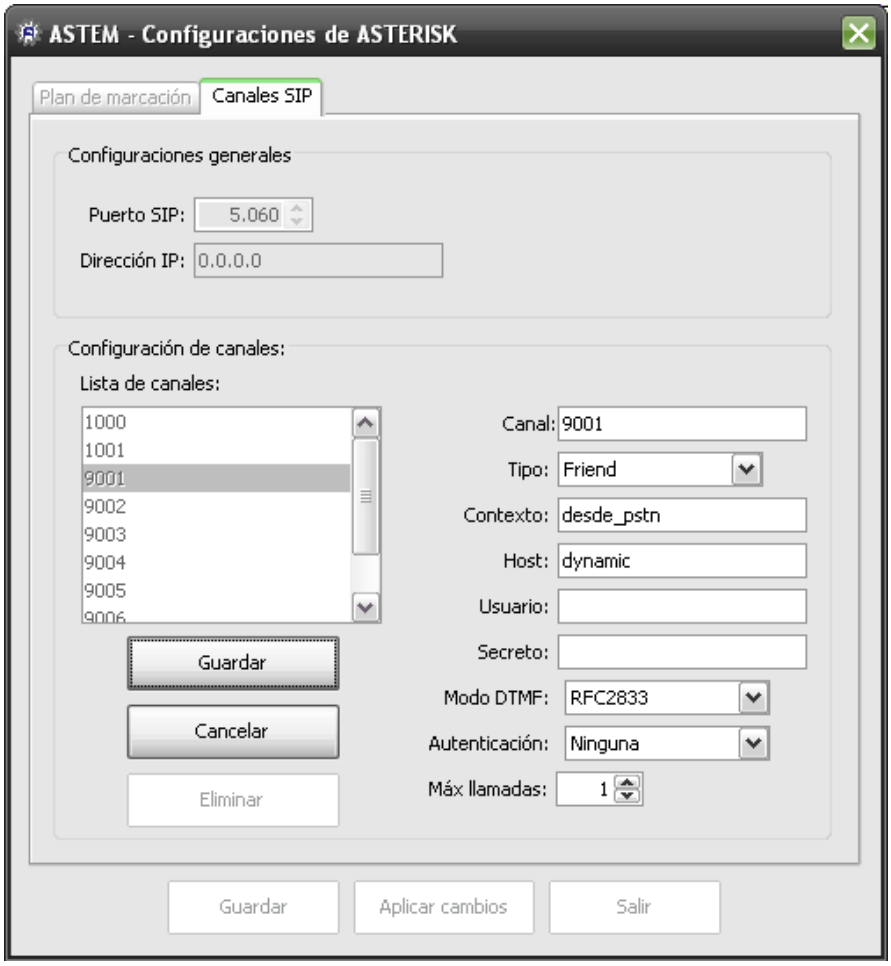


Figura 4.32. Ventana de configuración de canales SIP

7. Verificar que los datos hayan sido actualizados.

8. Guardar y aplicar la configuración en los archivos de ASTERISK.

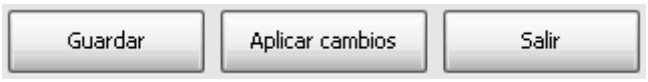


Figura 4.33. Botones de acción de la ventana de configuraciones de ASTEM

9. Cerrar la ventana de configuración de ASTERISK.

10. Comprobar que la nueva configuración se ejecuta en la PBX.

Resultados:

- A través de la ventana de configuración de la PBX se pudo modificar algunos aspectos de los archivos de ASTERISK. Estos archivos fueron

guardados con éxito por el sistema, y los cambios fueron aplicados correctamente en la PBX.

- La pestaña de administración de canales SIP permitió agregar, eliminar y modificar los canales configurados. Esta opción es útil para configurar canales en un Gateway.

Observaciones:

- Al editar o agregar un canal SIP, las demás funciones se bloquean. Una vez terminada la actualización las funciones vuelven a estar disponibles.
- Los archivos de configuración utilizados por la PBX ASTERISK están programados para cumplir únicamente las funciones de la central y evitar que esta sea utilizada con otros fines.
- Cuando el sistema actualiza la configuración, reescribe los archivos de configuración de ASTERISK con los parámetros del sistema, por lo que es recomendado realizar cualquier modificación utilizando la ventana del sistema ASTEM. Caso contrario, los cambios efectuados podrán perderse al utilizar el sistema ASTEM.

4.1.5 GENERAR LLAMADAS DE PRUEBA A UN NÚMERO DE DESTINO

Propósito:

- Realizar varias llamadas de prueba utilizando un solo número destino.
- Comprobar el funcionamiento del generador individual de llamadas.

Contexto:

En el lado del servidor, se encuentra instalada y configurada adecuadamente la PBX ASTERISK para recibir llamadas de lazo cerrado a través de una tarjeta de telefonía analógica de 4 puertos. Además, la PBX se encuentra configurada para recibir conexiones a través de “Asterisk Manager”. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de generación de llamadas individuales.

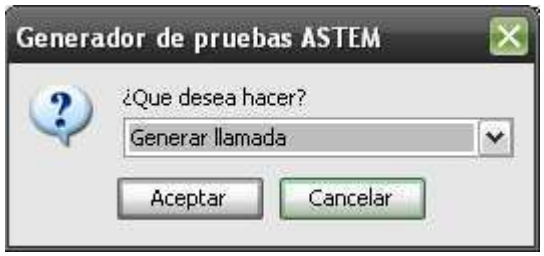


Figura 4.34. Menú de ingreso a la ventana de generación de llamadas

3. Seleccionar la tarjeta BESAME-NY-9, la troncal DAHDI/1 y el destino 88928312 para iniciar las pruebas de lazo cerrado.

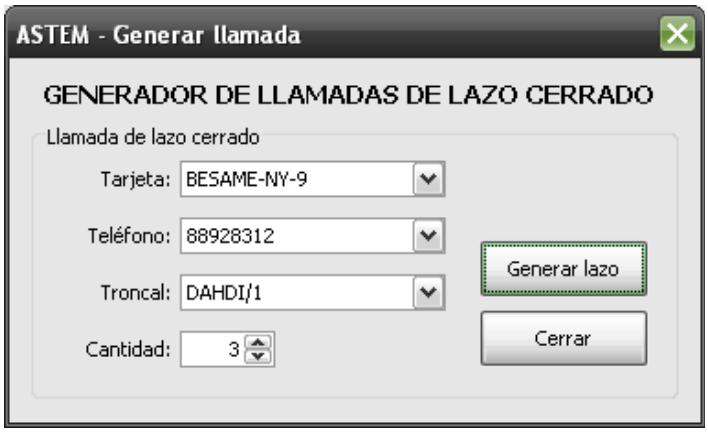


Figura 4.35. Opciones de generación de llamadas individuales

4. Definir la cantidad de pruebas en 3 e iniciar las pruebas.
5. Verificar el mensaje de confirmación recibido.

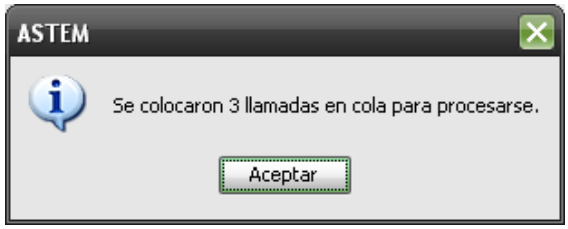


Figura 4.36. Mensaje de confirmación de llamadas iniciadas

6. Visualizar el proceso de ejecución de llamadas en la consola de la PBX ASTERISK.

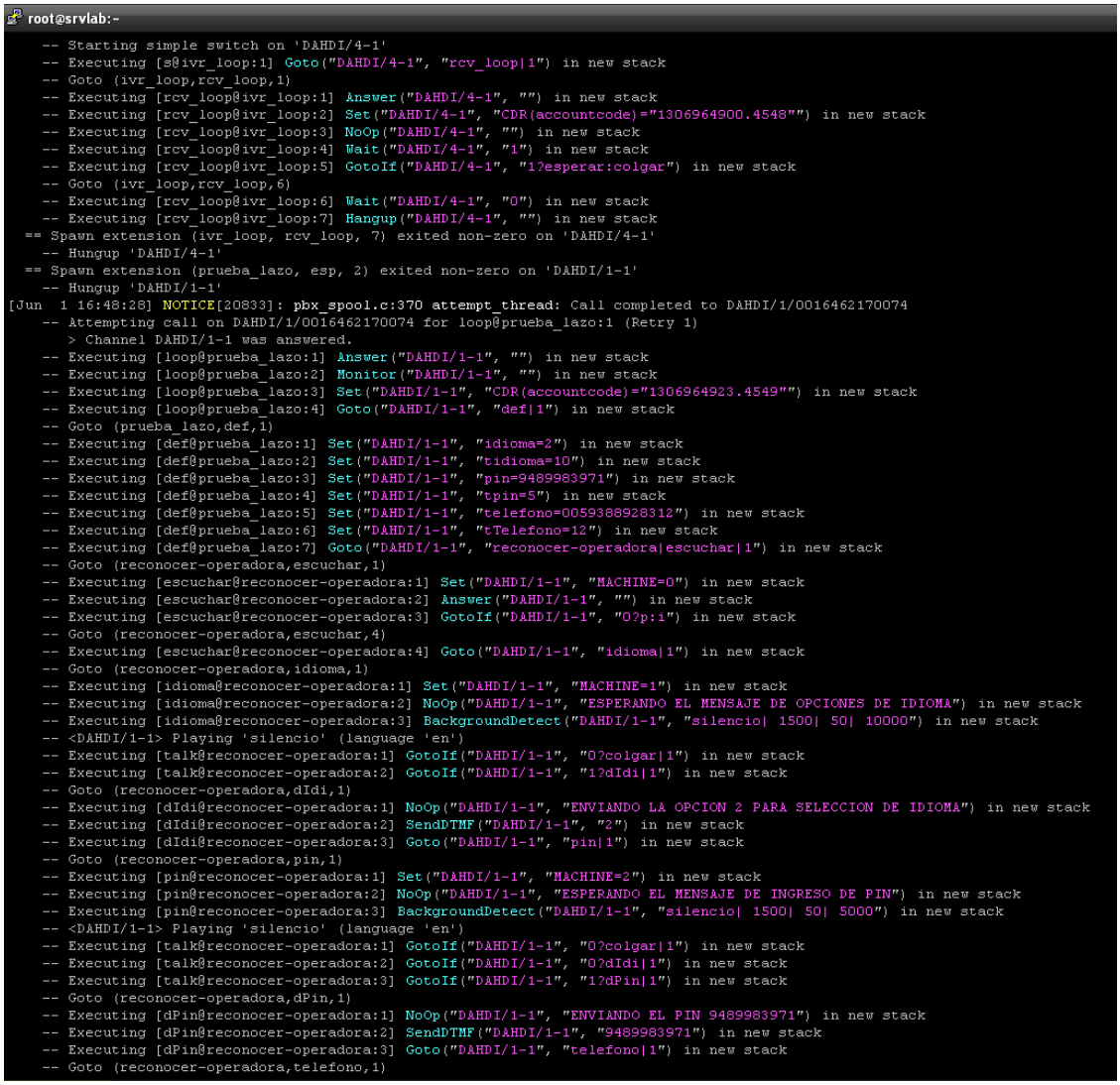


Figura 4.37. Eventos de inicio de la segunda llamada en la PBX

7. Verificar que las 3 llamadas de prueba sean recibidas en el sistema.

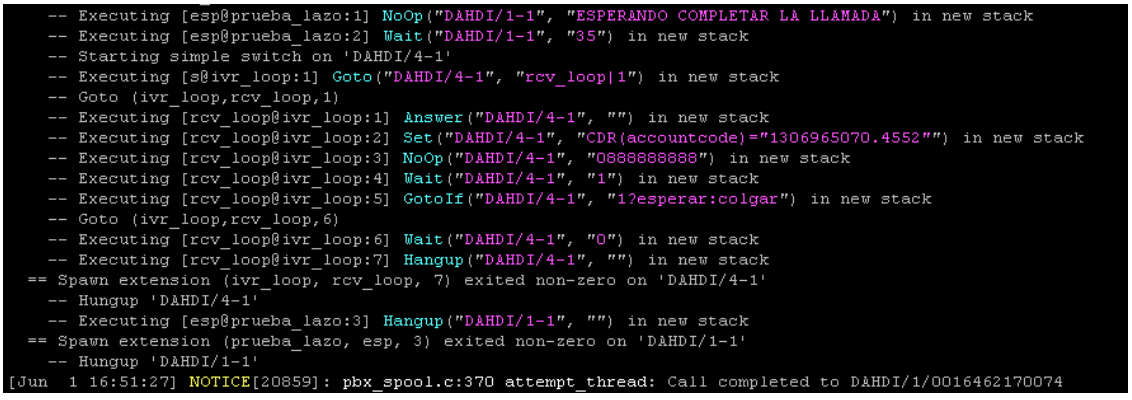


Figura 4.38. Eventos de terminación de la segunda llamada en la PBX

Resultados:

- Las 3 llamadas de prueba colocadas en la cola se completaron sin problemas. Las llamadas se ejecutaron de forma consecutiva, es decir, una tras otra acorde al tiempo configurado para cada llamada.
- Se pudo observar en la consola de ASTERISK el procedimiento de cada llamada luego de que ha sido contestada por la operadora automática. Se pudo constatar que el sistema espera hasta que la grabadora deje de hablar para enviar el siguiente comando.
- Las tres llamadas originadas en la prueba se recibieron exitosamente en el sistema. Esta prueba no generó ningún número sospechoso, sin embargo, se recibieron dos *Caller ID* en blanco y uno con código 088888888.

Observaciones:

- En algunas ocasiones las operadoras de telefonía transmiten *Caller ID* sin información o con la etiqueta *Privado*, lo cual no permite verificar la ruta a través de la cual ingresó una llamada.

4.1.6 PROGRAMAR UN GRUPO DE LLAMADAS DE PRUEBA

Propósito:

- Realizar varias llamadas de prueba utilizando un grupo de troncales configuradas en la PBX ASTERISK.
- Comprobar el funcionamiento del programador de llamadas de lazo cerrado.

Contexto:

En el lado del servidor, se encuentra instalada y configurada adecuadamente la PBX ASTERISK para recibir llamadas de lazo cerrado a través de una tarjeta de telefonía analógica de 4 puertos. Además, la PBX se encuentra configurada para recibir conexiones a través de “Asterisk Manager” y para guardar la información de los CDR’s recibidos en una base de datos en MySQL. Basándose en las

condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la opción “Generar pruebas” en el menú “Llamadas”.

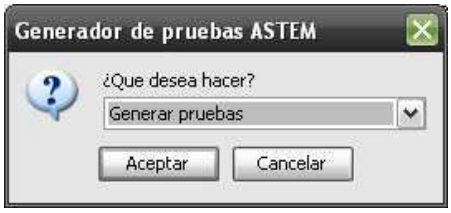


Figura 4.39. Opción “Generar pruebas”

3. Seleccionar las tarjetas COPA-1RO-4 y COPA-1RO-5; las troncales DAHDI/1 y DAHDI/2; y los números 088928312 y 095776760 con dos llamadas a cada uno para las pruebas de lazo cerrado.

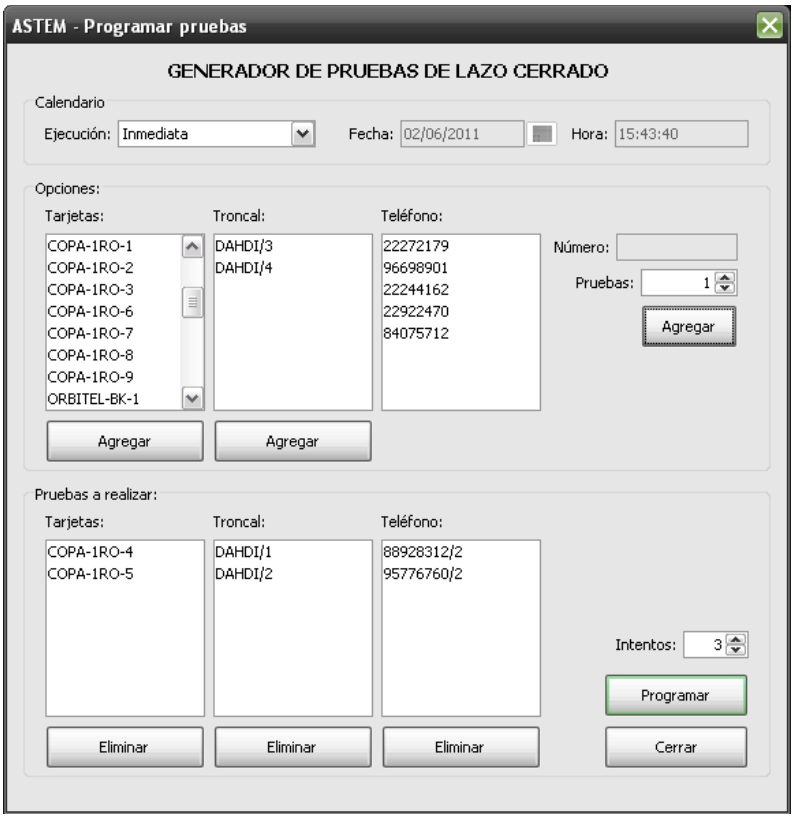


Figura 4.40. Generador de grupos de pruebas de lazo cerrado

4. Seleccionar la ejecución como inmediata e iniciar las pruebas.

5. Observar los archivos creados en la carpeta “/var/spool/astem”

Figura 4.41. Carpetas creadas en el directorio temporal del sistema

6. Visualizar el proceso de ejecución de llamadas en la consola de la PBX ASTERISK.

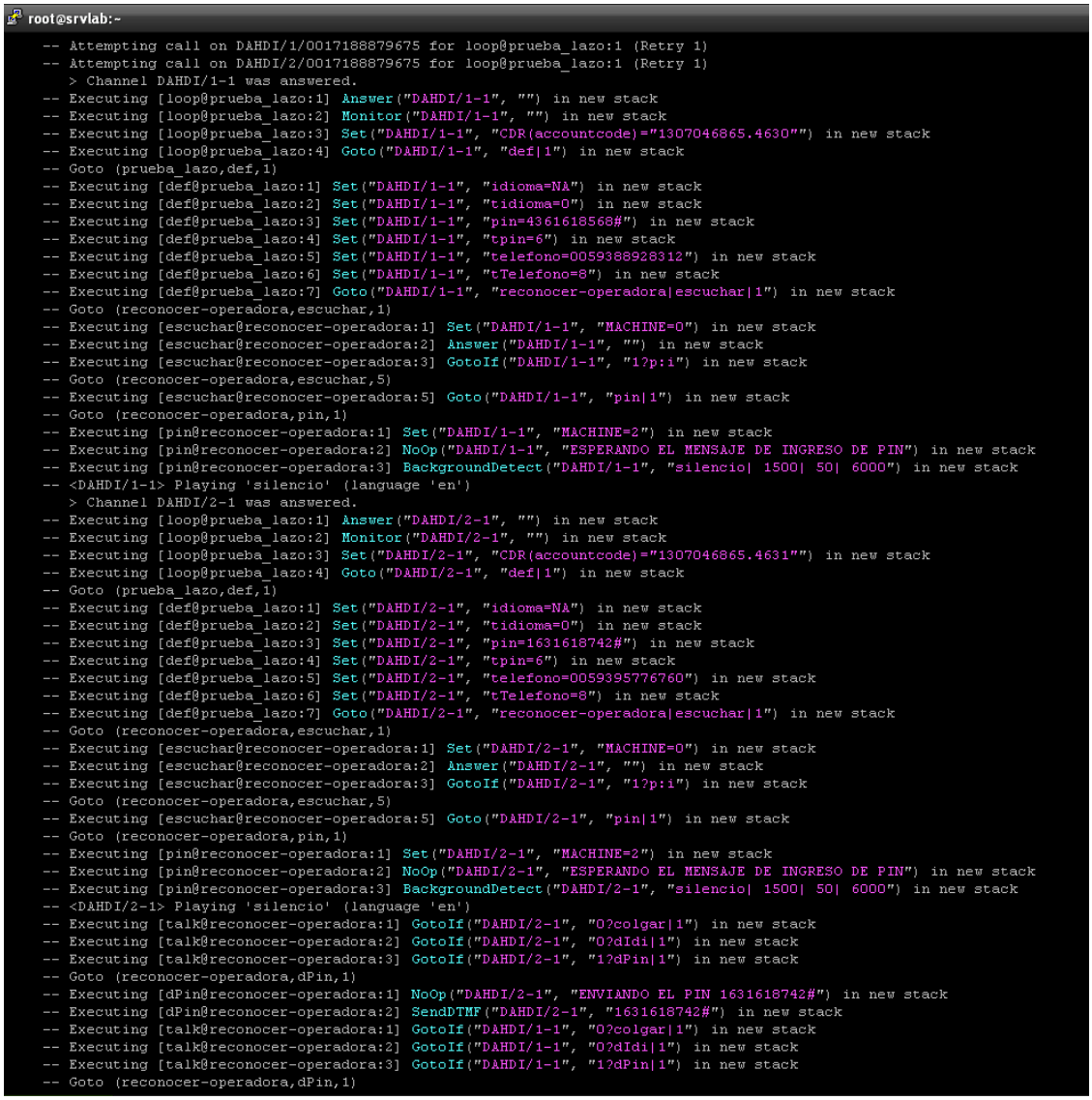


Figura 4.42. Inicio del grupo de pruebas con 2 llamadas simultáneas

7. Verificar que todas las llamadas de prueba sean recibidas en el sistema.

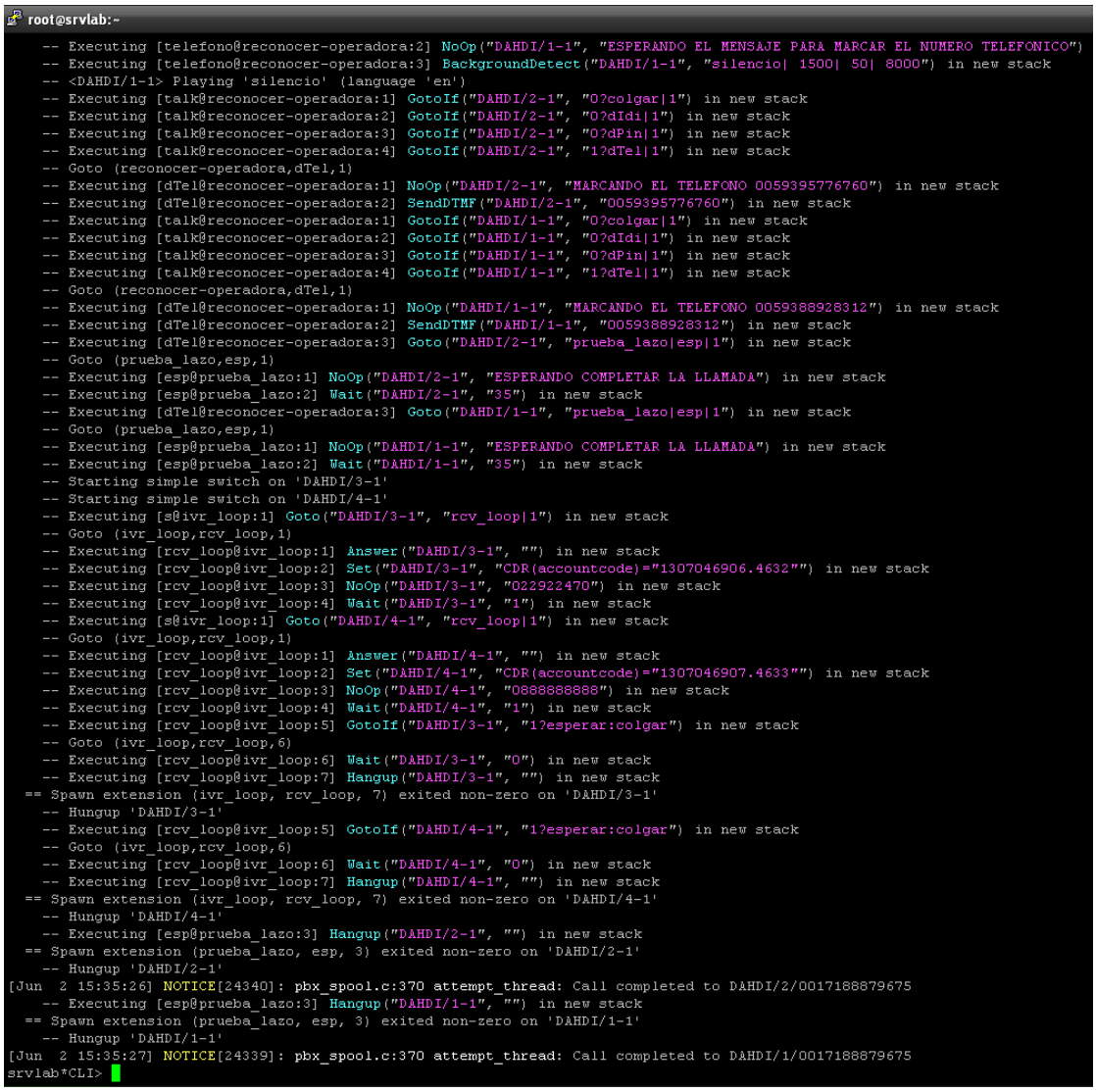


Figura 4.43. Recepción del segundo par de llamadas de prueba

8. Ingresar a la ventana de programación de pruebas de lazo cerrado.

9. Seleccionar las mismas tarjetas, troncales y números destino que se seleccionó en el literal 3.

10. Seleccionar la ejecución como programada y definir una hora y fecha para las llamadas. Iniciar las pruebas.

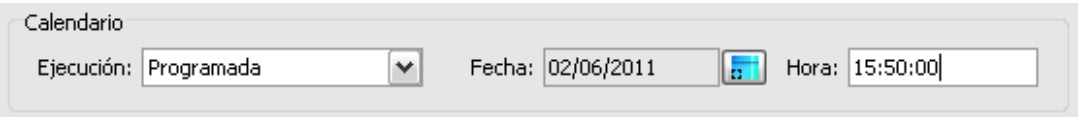


Figura 4.44. Configuración de fecha y hora para las llamadas de prueba

11. Una vez que se llegue a la fecha y hora indicada, observar los archivos creados en la carpeta “/var/spool/astem”.

12. Visualizar el proceso de ejecución de llamadas en la consola de la PBX ASTERISK.

13. Verificar que todas las llamadas de prueba sean recibidas en el sistema.

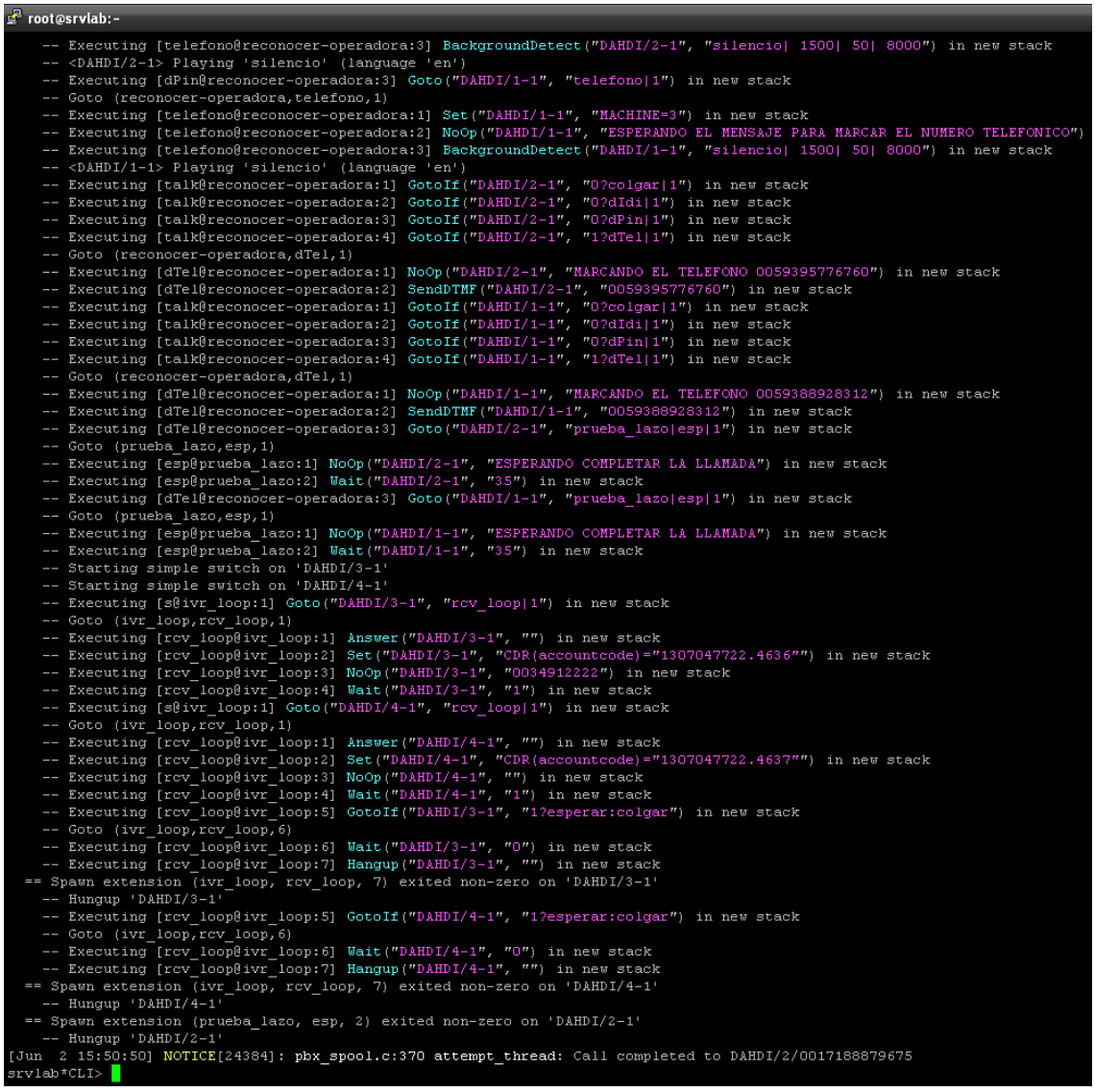


Figura 4.45. Recepción del par de llamadas de las pruebas programadas

Resultados:

- Los grupos de llamadas generados a través del sistema se ejecutaron con éxito y fueron recibidas por la PBX. Se pudo comprobar que la PBX realizó 2 llamadas simultáneamente.

- Se ejecutaron llamadas programadas a 5 minutos en el futuro. Una vez que llegó la hora programada, el sistema automáticamente inició el proceso de llamada con la PBX. Estas llamadas de igual forma fueron realizadas y recibidas con éxito.

Observaciones:

- Si se realizan llamadas de lazo cerrado utilizando una tarjeta de telefonía analógica de 4 puertos FXO, como en estas pruebas, únicamente se pueden realizar 2 llamadas simultáneas ya que se necesita un par de líneas por cada llamada. Si se realizan llamadas de lazo abierto, se pueden realizar hasta 4 llamadas utilizando los 4 puertos de la tarjeta.

4.1.7 IDENTIFICAR EL CAMPO DE CALLER ID EN UNA LLAMADA DE LAZO CERRADO

Propósito:

- Recibir una llamada de lazo cerrado y contestarla en la PBX.
- Verificar el campo en el cual la PBX identifica el *Caller ID*.

Contexto:

En el lado del servidor, se encuentra instalada y configurada adecuadamente la PBX ASTERISK para recibir llamadas de lazo cerrado a través de una tarjeta de telefonía analógica de 4 puertos.

Figura 1.46. Diagrama de los equipos utilizados en este escenario

Se inicia una llamada de lazo cerrado hacia un número fijo y esta llamada es recibida y contestada por la PBX. La PBX direcciona la llamada hacia la 1000 y luego de 3 segundos cierra la llamada.

A la red se ha conectado un equipo analizador de protocolos, marca SUNRISE TELECOM, que recibirá todos los paquetes de VoIP que circulen por la red. En la Figura 1.46 se observa el diagrama de la red. El analizador de protocolos recibirá el mensaje SIP de la PBX hacia la extensión 1000 que contiene el *Caller ID* de la prueba de lazo cerrado, y generará un CDR.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de generación de llamadas individuales.
3. Seleccionar la tarjeta COPA-1RO-2, la troncal DAHDI/1 y el destino 2922470 para iniciar la prueba de lazo cerrado.
4. Verificar que la prueba se llevó a cabo exitosamente. La PBX debe contestar la llamada y el *soft phone* en la extensión 1000 debe timbrar una o dos veces.
5. Extraer la información capturada por el analizador de protocolos.
6. Verificar el CDR generado en el analizador de protocolos por los mensajes SIP.

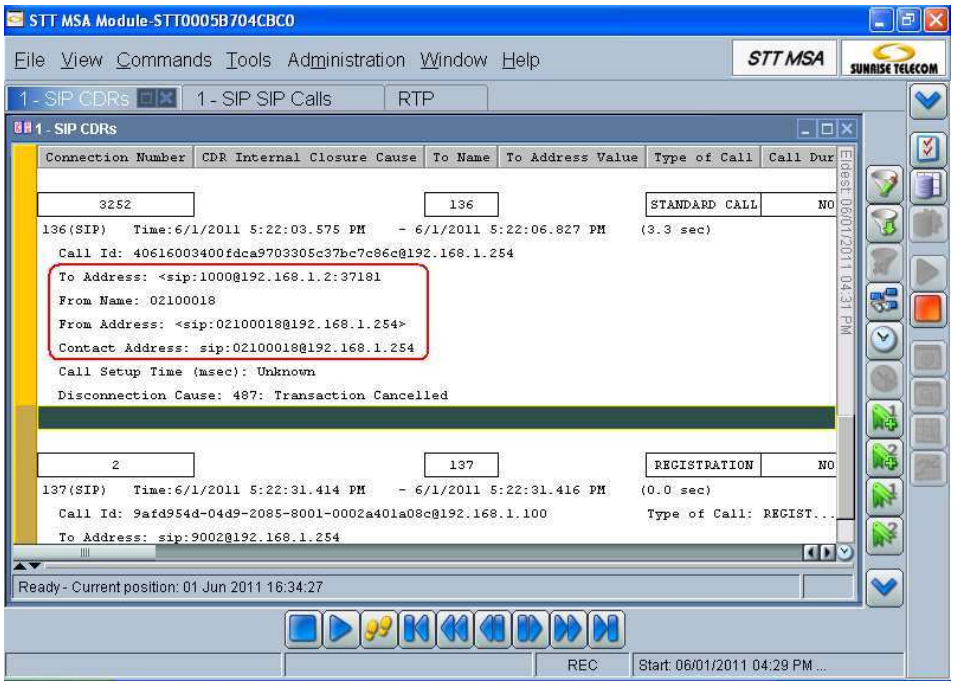
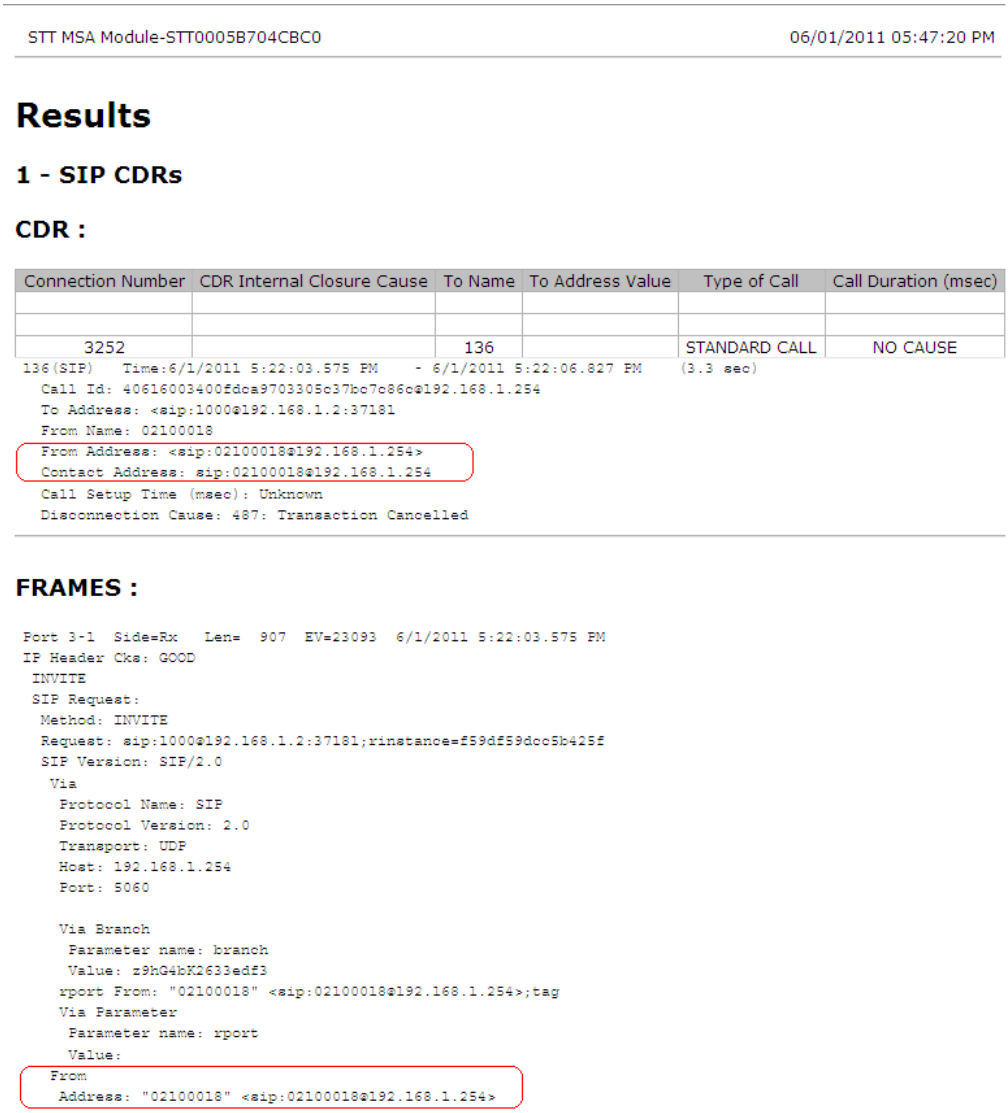


Figura 1.47. Imagen del CDR generado por el analizador de protocolos

7. Verificar el mensaje *INVITE* capturado por el analizador de protocolos, y el *Caller ID* en el mensaje.



STT MSA Module-STT0005B704CBC0 06/01/2011 05:47:20 PM

Results

1 - SIP CDRs

CDR :

Connection Number	CDR Internal Closure Cause	To Name	To Address Value	Type of Call	Call Duration (msec)
3252		136		STANDARD CALL	NO CAUSE

136(SIP) Time:6/1/2011 5:22:03.575 PM - 6/1/2011 5:22:06.827 PM (3.3 sec)
Call Id: 40616003400fdca9703305c37bc7c86c@192.168.1.254
To Address: <sip:1000@192.168.1.2:37181
From Name: 02100018
From Address: <sip:02100018@192.168.1.254>
Contact Address: sip:02100018@192.168.1.254
Call Setup Time (msec): Unknown
Disconnection Cause: 487: Transaction Cancelled

FRAMES :

Port 3-1 Side=Rx Len= 907 EV=23093 6/1/2011 5:22:03.575 PM
IP Header Cks: GOOD
INVITE
SIP Request:
Method: INVITE
Request: sip:1000@192.168.1.2:37181;rinstance=f59df59dcc5b425f
SIP Version: SIP/2.0
Via
Protocol Name: SIP
Protocol Version: 2.0
Transport: UDP
Host: 192.168.1.254
Port: 5060

Via Branch
Parameter name: branch
Value: z9hG4bK2633edf3
rport From: "02100018" <sip:02100018@192.168.1.254>;tag
Via Parameter
Parameter name: rport
Value:
From
Address: "02100018" <sip:02100018@192.168.1.254>

Figura 1.48. Imagen del mensaje capturado por el analizador de protocolos

Resultados:

- La llamada fue recibida y contestada en la PBX. Luego de contestada fue direccionada a la extensión 1000 y después de 3 segundos terminó la llamada.

- Se pudo constatar en el analizador de protocolos el mensaje *INVITE* de SIP capturado y sus campos. En especial su campo de *Caller ID* denominado "*From Name*" en el mensaje. Adicionalmente, en el mensaje

INVITE se construye el campo "*From Address*" utilizando el *Caller ID* y la dirección IP de la PBX.

- El sistema analiza este campo recibido desde el operador nacional para identificar si la llamada se debe considerar como sospechosa o no. En este caso se puede observar el código 0210001 correspondiente a un *carrier* internacional por lo que la llamada es identificada como normal.

Observaciones:

- En ciertas ocasiones puede ser necesario solicitar a las operadoras los CDR's de los números a los que se realizaron llamadas de prueba. La operadora CNT genera CDR's únicamente de las llamadas contestadas, por lo que es necesario que llamadas de prueba a esta operadora sean contestadas. Los demás operadores generan CDR's desde que la línea comienza a timbrar, por lo que no hace falta contestar la llamada.
- Se debe considerar que contestar una llamada implica utilizar saldo disponible en las tarjetas pre-pago, por lo que se puede realizar menos pruebas con una misma tarjeta si las llamadas son contestadas.

4.1.8 IDENTIFICACIÓN DE ALERTAS Y ENVÍO DE NOTIFICACIONES

Propósito:

- Verificar el funcionamiento del monitor del sistema ASTEM.
- Verificar la conexión con el servidor de correo electrónico.
- Enviar un correo electrónico automático al recibir una llamada desde un número telefónico nacional.
- Comprobar que las notificaciones son registradas en la base de datos.

Contexto:

Se utilizará una línea telefónica fija que no se encuentra conectada a la PBX para realizar una llamada hacia la misma. La PBX se encuentra configurada para realizar y recibir llamada a través de un Gateway telefónico. La aplicación servidor

ASTEM se encuentra ejecutando el monitor de la PBX y para guardar la información de los CDR's recibidos en una base de datos en MySQL. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de Estado del Servidor.
3. Comprobar que el monitor se encuentra en ejecución. Iniciarlo si es necesario.
4. Cerrar la ventana de Estado del Servidor.
5. Realizar pruebas hasta recibir resultados.
6. Ingresar a la cuenta de correo electrónico configurada para recibir notificaciones.

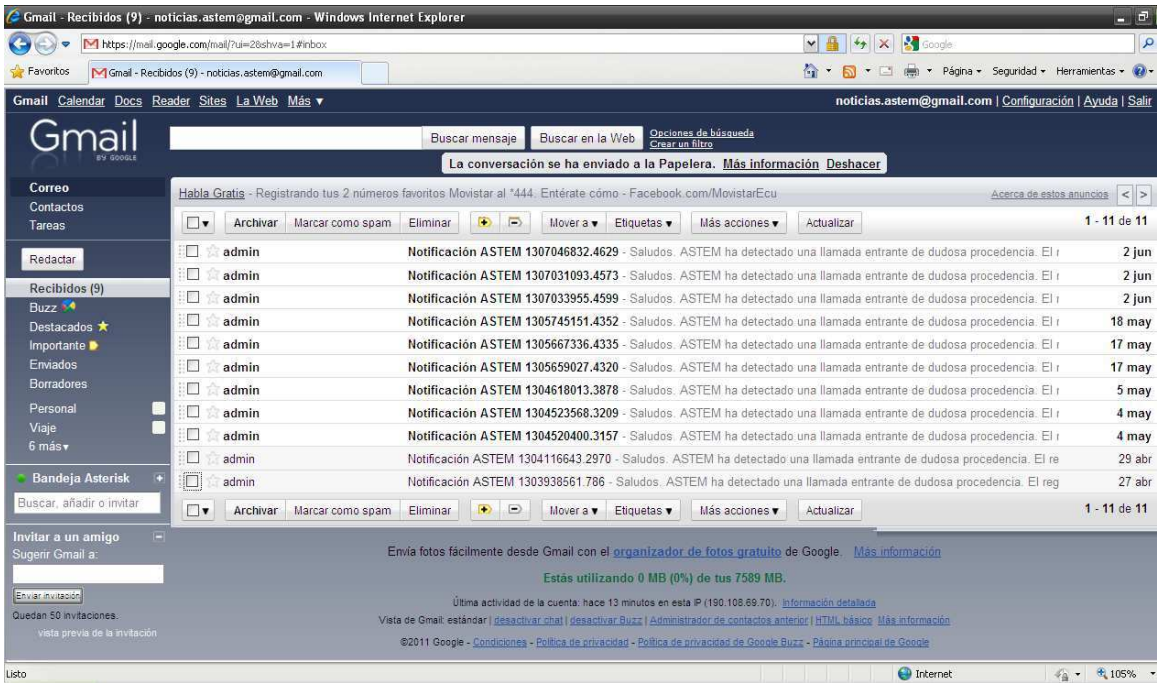


Figura 4.49. Imagen de alertas enviadas por el sistema vía correo electrónico

7. Comprobar que el correo electrónico de notificación fue recibido correctamente.

Figura 4.50. Correo electrónico generado por el sistema

8. Ingresar a la base de datos de MySQL y comprobar que la notificación fue registrada.

Resultados:

- Se realizaron varias llamadas de lazo durante las pruebas y se logró obtener varios números sospechosos, los cuales identificó el sistema y emitió la alerta correspondiente a través del correo electrónico.

- Se pudo comprobar la conexión con el servidor de correo electrónico y el registro del evento en la base de datos. La base de datos del sistema registra por separado la identificación de los números sospechosos y el envío del correo electrónico respectivo. En la Figura 4.50 se pueden observar las dos columnas correspondientes a la identificación del número sospechoso (penúltima columna de la derecha) y el envío del correo electrónico de alerta (última columna de la derecha); el número 1 indica un resultado positivo (verdadero), el 0 indica resultado negativo (falso).

Observaciones:

- Para todas las llamadas de prueba, existe una ventana de tiempo determinada por el sistema, durante la cual espera recibir una llamada. Esta ventana de tiempo está ligada al tiempo entre llamadas y la duración máxima de una llamada de prueba.

4.1.9 REALIZAR UNA CONSULTA A LOS CDR DE ASTEM

Propósito:

- Realizar una consulta personalizada en la base de datos de notificaciones del sistema.
- Manejar la información recibida de una consulta.
- Generar un reporte con la información seleccionada.

Contexto:

Se han realizado pruebas de lazo cerrado en escenarios anteriores, las cuales han sido registradas en la PBX. La PBX ha recibido llamadas desde números locales mientras el monitor del sistema se encontraba activo. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor), se realiza una consulta a la base de datos.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la opción “Base de datos” del menú principal.
3. Seleccionar la pestaña “CDR ASTEM”.
4. Seleccionar el tipo de consulta “Estándar”, el cual solicita los campos *Fecha de Inicio*, *Teléfono destino*, *Caller ID*, *Tarjeta* y *Costestada* a la base de datos del sistema.
5. Visualizar la información recibida desde la aplicación servidor.

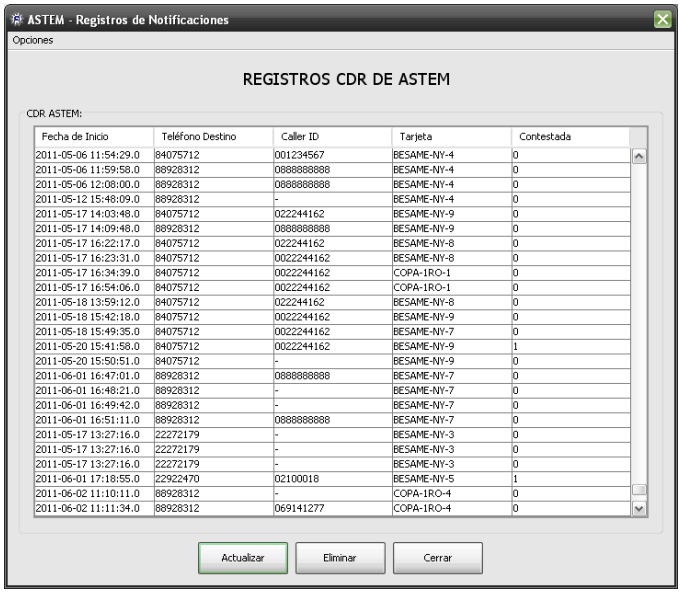


Figura 4.51. Información de una consulta “Estándar” devuelta por el servidor

6. Salir de la ventana de visualización.

7. Seleccionar el tipo de consulta “Personalizada”. Seleccionar un grupo de columnas a consultar, definir una condición y realizar la consulta.

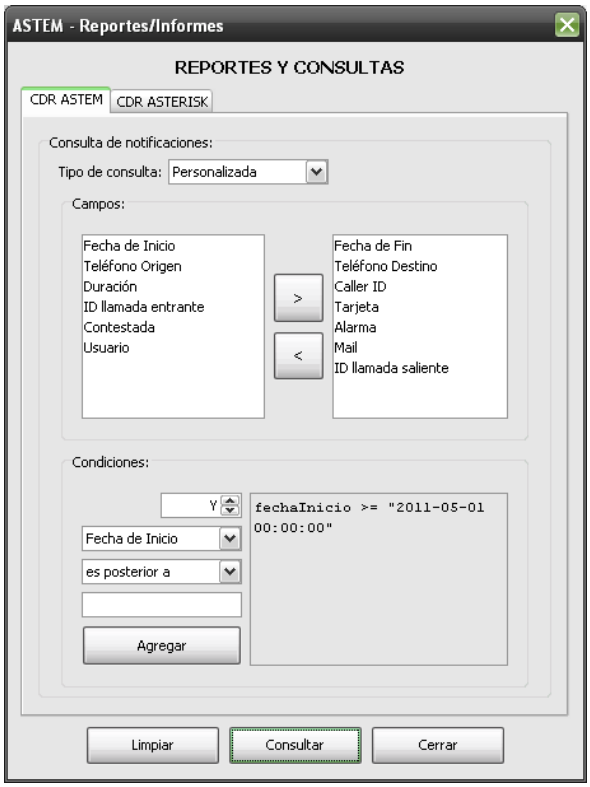


Figura 4.52. Ventana de definición de consultas a los CDR’s de ASTEM

8. Visualizar la información recibida desde la aplicación servidor.

Fecha de Fin	Teléfono Destino	Caller ID	Tarjeta	Alarma	Mail	ID llamada salie...
2011-05-04 09:46:45.0	22922470	062957038	BESAME-NY-2	1	1	-
2011-05-04 10:39:33.0	22922470	022244162	BESAME-NY-2	1	1	1304523563.3208
2011-05-04 11:16:14.0	22922470	02100018	BESAME-NY-3	0	0	1304525713.3240
2011-05-04 11:20:02.0	22922470	02100018	BESAME-NY-3	0	0	1304525942.3243
2011-05-04 11:22:42.0	22922470	02100018	BESAME-NY-3	0	0	1304526101.3247
2011-05-04 11:25:22.0	22922470	02100018	BESAME-NY-3	0	0	1304526261.3251
2011-05-04 11:29:23.0	22922470	02100018	BESAME-NY-3	0	0	1304526502.3256
2011-05-04 11:30:43.0	22922470	02100018	BESAME-NY-3	0	0	1304526582.3259
2011-05-04 11:32:06.0	22922470	02100018	BESAME-NY-3	0	0	1304526662.3262
2011-05-04 11:33:22.0	22922470	02100018	BESAME-NY-3	0	0	1304526742.3265
2011-05-04 11:36:05.0	22922470	02100018	BESAME-NY-3	0	0	1304526902.3269
2011-05-04 11:37:22.0	22922470	02100018	BESAME-NY-3	0	0	1304526981.3272
2011-05-04 11:38:43.0	22922470	02100018	BESAME-NY-3	0	0	1304527062.3275
2011-05-04 11:40:05.0	22922470	02100018	BESAME-NY-3	0	0	1304527142.3278
2011-05-04 11:41:26.0	22922470	02100018	BESAME-NY-3	0	0	1304527222.3281
2011-05-04 11:42:42.0	22922470	02100018	BESAME-NY-3	0	0	1304527302.3284
2011-05-04 11:44:05.0	22922470	02100018	BESAME-NY-3	0	0	1304527382.3287
2011-05-04 11:45:22.0	22922470	02100018	BESAME-NY-3	0	0	1304527462.3290
2011-05-04 11:48:04.0	22922470	02100018	BESAME-NY-3	0	0	1304527623.3294
2011-05-04 11:50:45.0	22922470	02100018	BESAME-NY-3	0	0	1304527783.3298
2011-05-04 11:52:02.0	22922470	02100018	BESAME-NY-3	0	0	1304527862.3301
2011-05-04 11:53:25.0	22922470	02100018	BESAME-NY-3	0	0	1304527942.3304
2011-05-04 11:54:43.0	22922470	02100018	BESAME-NY-3	0	0	1304528022.3307
2011-05-04 11:56:03.0	22922470	02100018	BESAME-NY-3	0	0	1304528103.3310
2011-05-04 11:57:23.0	22922470	02100018	BESAME-NY-3	0	0	1304528183.3313

Figura 4.53. Información devuelta por el servidor en una consulta personalizada a la base de datos de ASTEM

9. El botón “Eliminar” permite eliminar filas en la tabla que no contengan información útil.

10. Seleccionar el menú Opciones/Importar/Informe PDF.

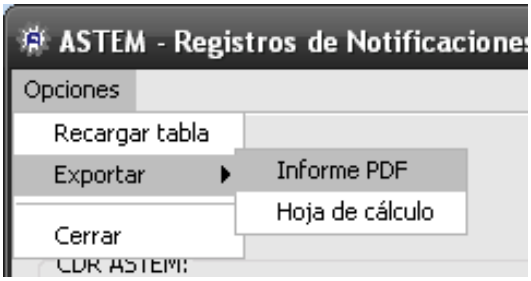


Figura 4.54. Menú de generación de reportes en PDF y hojas de cálculo

11. Seleccionar los márgenes y la ubicación del archivo.

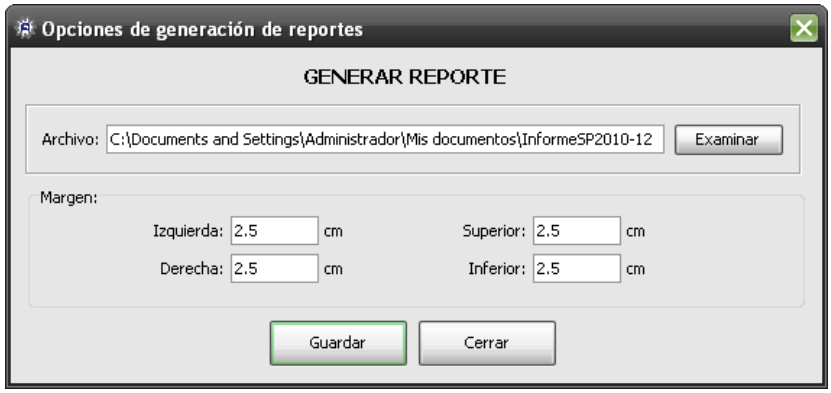


Figura 4.55. Imagen de las opciones de reporte

12. Generar un reporte con la información contenida en la tabla.

Figura 4.56. PDF generado por el sistema en base a la información de la base de datos de CDR de ASTEM

13. Repetir desde el literal 12, seleccionando la opción “Hoja de cálculo” en el menú “Exportar“.

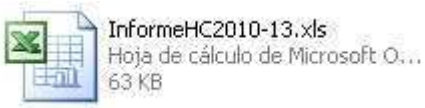


Figura 4.57. Hoja de cálculo generada por el sistema en base a la información de la base de datos de CDR de ASTEM

14. Salir de las ventanas de Reportes y Consultas.

Resultados:

- A través de la ventana de consultas fue posible acceder a la base de datos del sistema y recopilar información de las pruebas realizadas y sus resultados.
- La ventana permite realizar consultas “Estándar” que devuelven un grupo de parámetros definidos, o consultas “Personalizadas”, donde se pueden especificar los campos deseados y condiciones específicas de manera sencilla y rápida.

- La ventana de visualización permitió generar documentos PDF y una hoja de cálculo con la información mostrada. Las opciones de generación permiten personalizar los márgenes de los documentos PDF.

Observaciones:

- Cuando se genera una hoja de cálculo el sistema no permite realizar modificaciones a los márgenes del documento, ya que por defecto este no establece márgenes cuando lo crea.

4.1.10 REALIZAR UNA CONSULTA A LOS CDR DE ASTERISK

Propósito:

- Realizar una consulta personalizada en la base de datos de CDR de ASTERISK.
- Manejar la información recibida de una consulta.
- Generar un reporte con la información seleccionada.

Contexto:

Se han realizado pruebas de lazo cerrado en escenarios anteriores, las cuales han sido registradas en la PBX. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor) se establece la conexión con el servidor ASTEM utilizando la aplicación cliente para realizar una consulta a la base de datos.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar a la ventana de Reportes y Consultas en el botón registros.
3. Seleccionar la pestaña “CDR”.
4. Seleccionar el tipo de consulta “Estándar”, la cual solicita a la base de datos las columnas *Fecha y Hora*, *Caller ID*, *Origen*, *Duración*, y *Usuario* de todos los CDR’s.

5. Visualizar la información recibida desde la aplicación servidor.
6. Salir de la ventana de visualización.
7. Seleccionar el tipo de consulta “Personalizada”. Seleccionar un grupo de columnas a consultar, definir una condición de búsqueda y realizar la consulta.

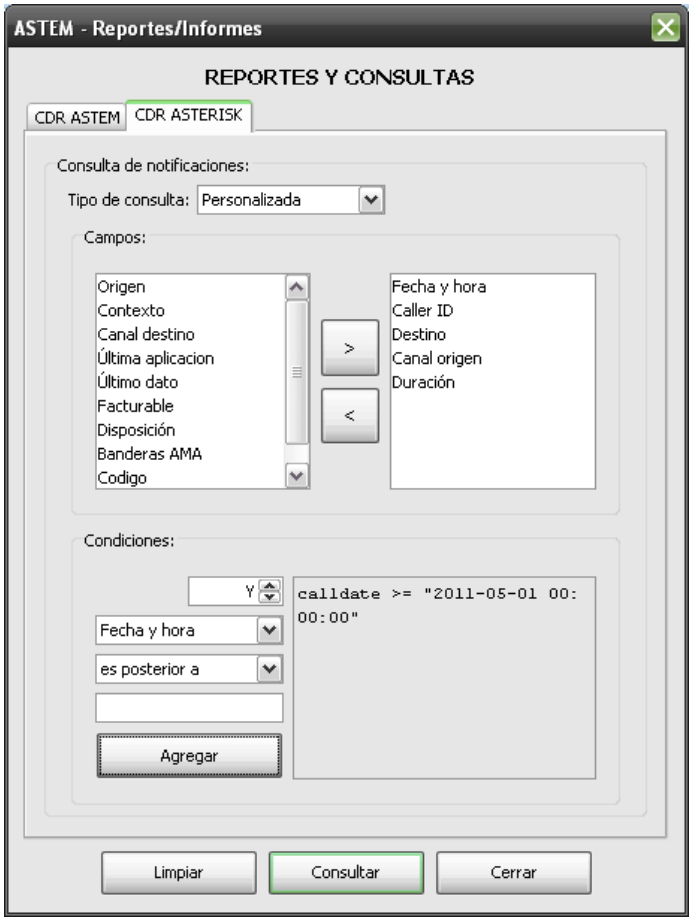


Figura 4.58. Ventana de definición de consultas a los CDR’s de ASTERISK

8. Visualizar la información recibida desde la aplicación servidor.
9. Salir de las ventanas de Reportes y Consultas.

Resultados:

- La ventana de consultas del sistema ASTEM permitió realizar las consultas a la base de datos de CDR’s de ASTERISK propuestas. Los resultados se pudieron visualizar, verificando así el correcto funcionamiento de estas opciones.

Observaciones:

- Las funciones disponibles en la ventana de consulta de los CDR's de ASTERISK son las mismas que en la ventana de consulta de CDR's de ASTEM. Estas funciones fueron verificadas en el apartado 4.1.9.

4.1.11 DATOS ESTADÍSTICOS DEL SISTEMA

Propósito:

- Visualizar los resultados obtenidos de las pruebas realizadas en forma de gráficos estadísticos.
- Visualizar el estado del servidor y la cantidad de pruebas realizadas.

Contexto:

El sistema ha almacenado en su base de datos información respecto a las pruebas realizadas. Basándose en las condiciones del primer escenario (Conexión entre la aplicación cliente y servidor), se establece la conexión con el servidor ASTEM utilizando la aplicación cliente para realizar una consulta estadística de la información almacenada.

Procedimiento:

1. Conectarse a la aplicación servidor ASTEM utilizando el cliente.
2. Ingresar en la opción "Estadísticas".
3. Seleccionar en la lista de tarjetas la opción "Todas".
4. Seleccionar en el filtro de campos la opción "Caller ID".

Figura 4.59. Selección de parámetros generales para las estadísticas

5. Seleccionar la opción "Consultar" y verificar el gráfico.

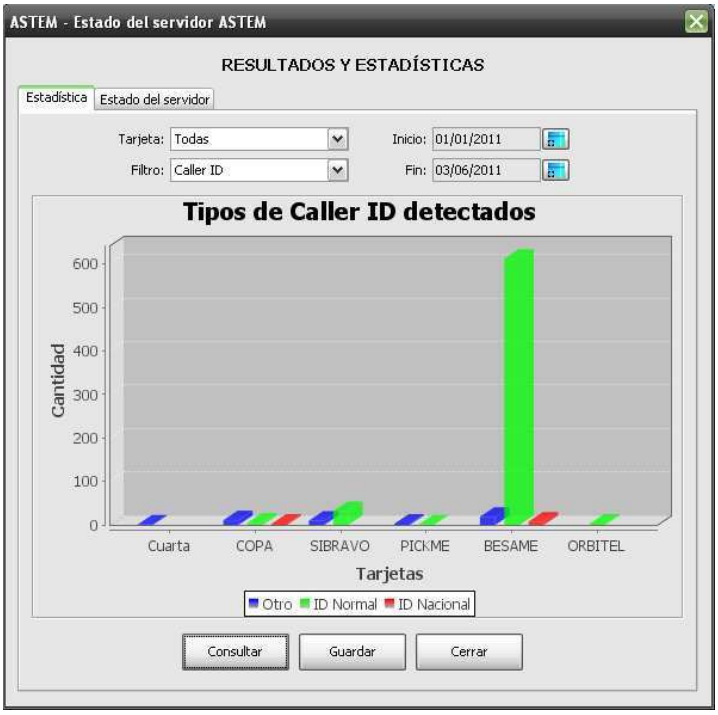


Figura 4.60. Datos estadísticos de todas las tarjetas en el sistema

6. Seleccionar en la lista de tarjetas la opción “BESAME”.

7. Seleccionar en el filtro de campos la opción “Caller ID”.

8. Seleccionar la opción “Consultar” y verificar el gráfico.

Figura 4.61. Datos estadísticos de las tarjetas “BESAME” en el sistema

9. Salir de la ventana de Estadísticas.

Resultados:

- El menú de Estadísticas del sistema permitió obtener datos sobre las pruebas completadas del sistema y sus resultados. Como se observa en las figuras, se puede apreciar los tipos de llamadas recibidas según la tarjeta, de forma general o individual.
- La opción “Guardar” permite guardar la imagen generada por el sistema en un archivo.

Observaciones:

- Al dar *click* sobre la imagen generada por el sistema, esta se muestra en una ventana independiente donde es posible cambiar su tamaño, guardarla, realizar ampliaciones, entre otras cosas.
- El sistema genera estadísticas únicamente basándose en las tarjetas utilizadas en las llamadas de lazo cerrado. El sistema realiza una consulta específica a la base de datos, y en base a esa información genera los gráficos estadísticos.

4.1.12 REGISTROS DEL SISTEMA ASTEM

Propósito:

- Visualizar los mensajes de actividad registrados por el sistema.

Contexto:

Utilizando el sistema han realizado pruebas de lazo cerrado, y se han realizado cambios en la configuración y en las opciones de tarjetas. Durante las pruebas realizadas el sistema ha cumplido diferentes tareas. Se ingresa al servidor del sistema para tener acceso a los archivos de registro del sistema ASTEM.

Procedimiento:

1. Ingresar al servidor del sistema.

2. Ingresar a la carpeta “/var/log/”

3. Ingresar al archivo “astemlog”

4. Visualizar lo mensajes de actividad del sistema ASTEM.

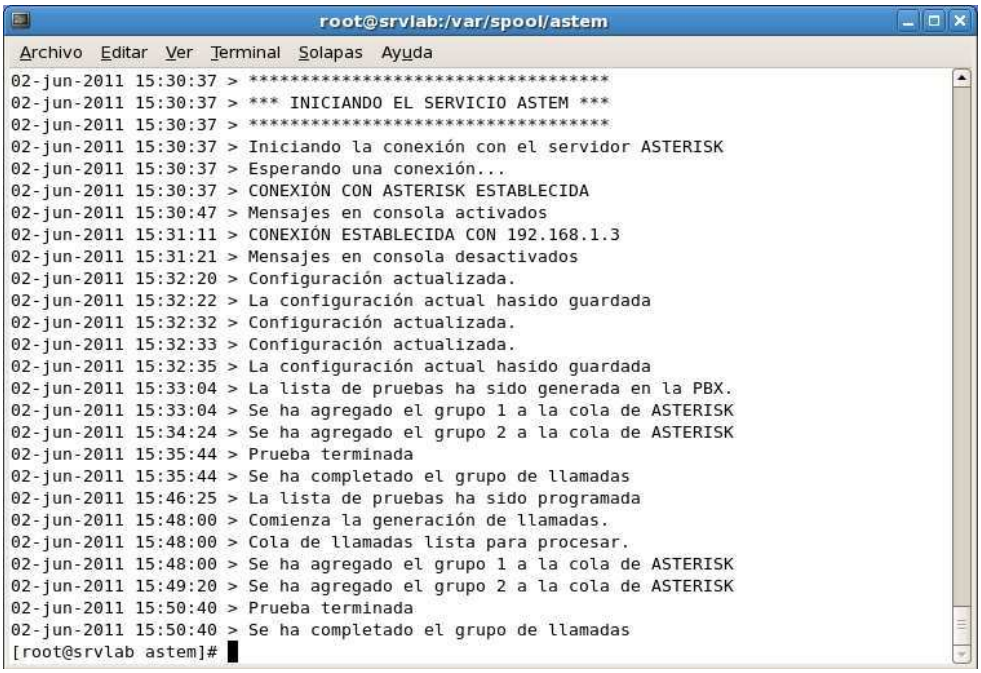


Figura 4.62. Eventos almacenados en los logs del sistema

Resultados:

- En el archivo se encuentra registrado todos los eventos que se producen en el sistema, incluyendo cambios en las configuraciones o en el archivo de tarjetas. El archivo de registros nunca es sobrescrito, aunque se reinicie el sistema.

- El sistema permite activar o desactivar los mensajes en pantalla utilizando el comando “debug”. Adicionalmente, el sistema se encuentra diseñado para que solo guarde la información relativa a eventos del sistema.

Observaciones:

- La cantidad de información almacenada en este registro puede llegar a ser muy grande y ocupar demasiado espacio en el disco duro.

4.2 BENEFICIOS Y LIMITACIONES DEL SISTEMA

4.2.1 BENEFICIOS ECONÓMICOS

El sistema, por ser una aplicación desarrollada en la SUPERTEL, representa un ahorro económico para la SUPERTEL. Es necesario destacar que el sistema es una solución enfocada a satisfacer las necesidades de la SUPERTEL, lo cual es una ventaja frente a soluciones comerciales que difícilmente cumplen con todos los requerimientos. Esto, económicamente hablando, implica que la SUPERTEL no debe invertir en funcionalidades adicionales que sean necesarias ya que todas se encuentran implementadas.

El costo final de desarrollo e implementación del sistema no es muy diferente de las soluciones comerciales más comunes, sin embargo, no es necesario adquirir o renovar la licencia para su utilización. Además, los usuarios están en capacidad de añadir funcionalidades o cambiar sus características según considere necesario, sin necesidad de parches o actualizaciones.

En cuanto a hardware, el sistema no requiere de equipos adicionales para añadir funcionalidades o agregar más líneas de prueba, únicamente es necesario agregar tarjetas de telefonía analógicas; por otro lado, en soluciones comerciales, es necesario adquirir más equipos si se desea aumentar la capacidad del sistema, lo cual implica mayores costos. Todos estos detalles representan beneficios económicos para la SUPERTEL y el estado Ecuatoriano.

4.2.2 BENEFICIOS EN TIEMPO

Sin duda, los beneficios en tiempo son sencillos de determinar. El sistema que la SUPERTEL utiliza actualmente es capaz de realizar una llamada cada 2 minutos aproximadamente, lo cual representa un promedio de 30 llamadas por hora, en el mejor de los casos. En sistema ofrece la posibilidad de generar llamadas simultáneas. En este trabajo se realizaron hasta 2 llamadas simultáneas con un tiempo de 1.5 minutos por llamada aproximadamente, lo cual significa un promedio ideal de 80 llamadas por hora. La solución comercial termina una llamada cada 2 minutos, mientras que el sistema lo hace cada 45 segundos. [15]

Como se puede observar, el tiempo de una llamada de prueba utilizando el sistema desarrollo es significativamente menor, y esto por ende, es un ahorro de tiempo para la SUPERTEL ya que puede realizar más del doble de llamadas de prueba en el mismo periodo de tiempo.

Adicionalmente, el sistema puede ser ampliado para realizar más llamadas simultáneas sin necesidad de realizar cambios significativos. Para esto es necesario instalar una tarjeta analógica de mayor capacidad y configurarla en el sistema para que la utilice.

4.2.3 BENEFICIOS FUNCIONALES

Los beneficios funcionales parten de los requerimientos que el programa satisface, y las funciones adicionales que implementa. El sistema tiene la facilidad de generar múltiples llamadas simultáneas; el número de llamadas que se podrían realizar depende del número de puerto que la tarjeta de telefonía analógica conectada tenga, en este caso 4. Además, el sistema tiene la función de generar alertas vía correo electrónico, lo cual brinda un servicio adicional que permite a los funcionarios conocer las novedades durante las pruebas de forma casi inmediata.

El sistema, al ser propiedad de la SUPERTEL, puede ser corregido y adaptado a futuras necesidades. Si el programa llegará a presentar un problema de funcionamiento o configuración, la SUPERTEL tiene las herramientas necesarias para corregir el problema inmediatamente modificando algún detalle de programación.

Por ejemplo, si en algún momento fuera necesario cambiar la estructura en que se guardan las tarjetas de telefonía pre-pagada, se lo puede hacer reprogramando la clase correspondiente y compilando nuevamente el servidor.

La conexión remota es otra funcionalidad que beneficia su uso. A través de la aplicación cliente, el usuario puede acceder a las funcionalidades del servidor y la PBX sin requerir conocimientos avanzados de Linux o ASTERISK. Cabe recalcar que la facilidad que ofrece el sistema para aumentar la cantidad de llamadas simultáneas es superior a cualquier solución similar.

4.2.4 LIMITACIONES DEL SISTEMA

Pese a las mejoras que el sistema ofrece frente a otras soluciones similares, se pueden mencionar algunas limitaciones en el sistema. Las limitaciones son básicamente funciones adicionales que podrían añadirse al sistema.

Una vez que un número ha sido identificado como sospechoso, el sistema no identifica la operadora a la que pertenece. Para esto es necesaria una adecuada coordinación con las operadoras de telefonía a fin de que faciliten la numeración de líneas que tienen asignadas.

Por otro lado, el sistema no trabaja con portales WEB o programas de telefonía por Internet, como MSN, Skype, Google Talk, etc.

4.3 COSTO ESTIMADO DEL SISTEMA

El costo que una solución como la presentada en este trabajo puede tener en el mercado presenta una perspectiva general de la importancia de la misma. El costo del sistema está determinado principalmente por dos factores. En primer lugar, se debe tener en cuenta el costo de los equipos que son necesarios para su implementación, y en segundo lugar, el costo del diseño y desarrollo de la misma.

4.3.1 COSTO DE LOS EQUIPOS

En la Tabla 4.1 se detallan los equipos necesarios para la implementación del sistema y su valor en el mercado Ecuatoriano.

Equipo	Cantidad	Valor unitario (USD)	Valor (USD)
Servidor	1	800,00	800,00
Tarjeta de telefonía	1	350,00	350,00
Computador	1	800,00	800,00
Bases celulares	4	100,00	400,00
		Total:	2350,00

Tabla 4.1 Lista de equipos y su valor aproximado en el mercado.

La lista de equipos está basada en las especificaciones mínimas descritas en el Capítulo 3. El sistema incluye 4 bases celulares para realizar pruebas utilizando líneas de telefonía móvil; sin embargo, no incluye las líneas móviles ni fijas. El

sistema tampoco incluye elementos de red ya que posiblemente el sistema se instale sobre una red ya implementada.

4.3.2 COSTO DE DISEÑO E IMPLEMENTACIÓN

El diseño e implementación del sistema consta de dos etapas. En la primera se recopila información y diseña la solución; en la segunda, se realiza la implementación y pruebas de funcionamiento. En la Tabla 4.2 se observa el detalle del costo de diseño e implementación.

Motivo	Detalles	Valor (USD)
Diseño	80 horas/hombre Hora/hombre: 50 USD	4000,00
Desarrollo	650 horas/hombre Hora/hombre: 30 USD	24000,00
	Total:	28000,00

Tabla 4.2 Costos de diseño e implementación.

El costo de diseño está ligado directamente al trabajo de ingeniería que involucra la solución al problema; mientras que por otro lado, el desarrollo del mismo está determinado por las horas de trabajo necesarias para escribir el programa, solucionar problemas, e implementar el sistema en su totalidad para ponerlo en producción. Este es el paso final antes de la entrega.

4.3.3 COSTO TOTAL

El costo total del proyecto se estima sumando el valor de los equipos y el del desarrollo e implementación en la Tabla 4.3. Para este proyecto es importante recordar que no se utiliza software propietario, lo cual disminuye algunos costos.

Motivo	Valor (USD)
Equipos	2350,00
Diseño y desarrollo	28000,00
Subtotal:	30350,00
IVA:	3642,00
Total:	33992,00

Tabla 4.3 Costo final del desarrollo del sistema y equipos.

Para definir claramente una oferta completa para el desarrollo e implementación del sistema, se propone brindar capacitación de 40 horas en el uso del sistema a 4 empleados, un tiempo de implementación de 32 horas y 60 horas de soporte técnico a cualquier hora en el transcurso de un año. Se podría considerar una oferta con los valores de la Tabla 4.4.

Motivo	Número de horas	Precio (USD)	Monto
Instalación del sistema y pruebas	32	6,25	200,00
Capacitación	40	20,00	800,00
Soporte técnico	60	25,00	1500,00
CDs y manuales	-	-	25,00
		Subtotal:	2525,00
		IVA:	303,00
		Total:	2828,00

Tabla 4.4. Costos adicionales en la oferta del sistema.

Este monto se debe sumar al monto total de desarrollo y equipos del sistema para conocer el costo final de una propuesta con estas características. Estos valores se muestran en la Tabla 4.5.

Motivo	Valor (USD)
Equipos, diseño y desarrollo	33992,00
Implementación y soporte	2828,00
Total:	36820,00

Tabla 4.5 Costo final de una propuesta del sistema.

La oferta variará según los requisitos del cliente en cuanto a instalación, capacitación y soporte técnico.

4.3.4 COMPARACIÓN CON APLICACIONES COMERCIALES SIMILARES

En el mercado existe muy poca variedad de sistemas para automatizar llamadas de lazo cerrado. En algunos casos las operadoras interesadas desarrollan aplicaciones específicas para este propósito. Sin embargo, una aplicación llamada *SISPRIN* es una alternativa comercial utilizada por varios operadores de telefonía en el Ecuador.

4.3.4.1 Comparación de ASTEM con SISPRIN

El sistema SISPRIN está desarrollado para realizar llamadas de lazo cerrado utilizando módems telefónicos. Esta solución requiere de un computador y dos módems, que pueden ser teléfonos celulares, para cada pareja de líneas a utilizarse en una prueba de lazo cerrado. [15]

El sistema está desarrollado en 2 módulos principales, un módulo de generación de llamadas y uno de recepción. Cada módulo controla un módem encargado de iniciar o terminar una llamada. El sistema además implementa alertas en caso de recibir números sospechosos y permite generar reportes de su actividad. [15]

Característica	SISPRIN	ASTEM
Código	Propietario. Las modificaciones únicamente se realizan bajo consideración del fabricante.	Abierto. Cualquier modificación puede realizarse según las necesidades de la SUPERTEL.
Tipo de aplicación	Centralizada	Distribuida
Escalabilidad del software	Poco escalable. Nuevas funcionalidades implican un nuevo desarrollo y dependen de la compatibilidad del sistema.	Gran escalabilidad. Compatibilidad con tecnologías de VoIP y por ser código abierto permite agregar módulos según sea necesario.
Equipos	Un computador y un par de módems, o teléfonos celulares, por cada prueba de lazo cerrado.	Un servidor con tarjetas de telefonía analógica de hasta 24 puertos, es decir 12 llamadas de lazo cerrado por tarjeta. Permite añadir tarjetas de telefonía digital.
Escalabilidad de equipos	Un computador y un par de módems, o teléfonos celulares, por cada prueba de lazo cerrado que se desee adicionar.	Tarjetas de telefonía analógica adicionales con la cantidad de puertos requeridos.
Aumento de líneas telefónicas	Sujeta a la cantidad de computadores y módems disponibles.	Sujeta a la cantidad de puertos disponibles en la tarjeta del servidor.
Máximo número de líneas telefónicas	2 por computador	Sujeto a la cantidad de líneas en la(s) tarjeta(s) de telefonía del servidor
Generación de llamadas	Lazo cerrado y lazo abierto	Lazo cerrado y lazo abierto
Tipo de marcado	Por tiempos configurables	Escuchando la operadora

Alertas	Alerta visual	Alerta vía correo electrónico
Generación de Reportes	- Generación de llamadas con los datos de llamada - Reporte de llamadas realizadas por empresa - Total de llamadas desde la última puesta en marcha del sistema - Listado de tarjetas - Listado de *carriers* autorizados	- Generación de llamadas con los datos de llamada (CDR generado por el sistema) - Total de llamadas desde la última puesta en marcha del sistema - Total de llamadas solicitadas, generadas y completadas. - Estadísticas de los resultados de las pruebas.
Acceso al sistema	Interfaz gráfica.	Interfaz gráfica.
Configuración	Interfaz gráfica. Permite configurar opciones del programa y datos de tarjetas de telefonía pre-pagada.	Interfaz gráfica. Permite configurar opciones del sistema, opciones la base de datos, opciones del correo de alertas, opciones de la PBX ASTERISK y datos de tarjetas de telefonía pre-pagada.

Tabla 4.6. Características de los sistemas SISPRIN y ASTEM [15] [6]

En la Tabla 4.6 se observan una comparación entre las características de ambos sistemas. Como se puede observar, el sistema SISPRIN es mucho más cerrado y limitado que el sistema ASTEM, desarrollado en este trabajo. [6]

Detalle	SISPRIN	ASTEM
Diseño y desarrollo	5.000,00 (no incluye equipos)	33.992,00 (incluye equipos)
Implementación	Menor a 100.000,00	Menor a 40.000,00

Tabla 4.7. Costos de implementación de los sistemas ASTEM y SISPRIN [6]

En la Tabla 4.7 se observa una comparación aproximada de los costos de ambos sistemas, considerando una oferta del sistema ASTEM similar a la descrita en el apartado 4.3.3. Para esta comparación se tomó como referencia el precio al que la Corporación Nacional de Telecomunicaciones, o CNT, compró el sistema SISPRIN en el año 2007. [6]

Es evidente que la relación entre el costo de los sistemas y los beneficios que ofrecen señalan la solución desarrollada en este proyecto como una mejor opción por ser innovadora, eficiente, y proyectada para un funcionamiento a largo plazo.

4.4 APLICACIONES ADICIONALES

El sistema está diseñado exclusivamente para brindar una funcionalidad acorde con las necesidades de la SUPERTEL. Sin embargo, sus módulos y funciones pueden tener otras aplicaciones, además que pueden ser la base para nuevas funciones del sistema.

En el campo del combate a los ilícitos en telecomunicaciones, se puede agregar la función de generar llamadas de lazo cerrado a través de portales WEB o números DID, lo que permitiría cubrir mayor número de posibles fuentes de llamadas no autorizadas. El sistema realizaría el mismo proceso de recepción y generación de CDR, aunque el método utilizado para generar las llamadas será diferente.

Adicionalmente, las funciones que la PBX ASTERISK realiza pueden ser utilizadas para generar llamadas automáticas conocidas como tele-mercadeo. Utilizando la misma estructura definida para generar las llamadas de lazo cerrado, se puede configurar la PBX para que reproduzca un mensaje o difunda información a través de llamadas aleatorias automáticas. Este servicio suele ser utilizado por empresas para realizar marketing o promocionar productos y servicios.

4.5 EL FUTURO DEL SISTEMA ASTEM

La Superintendencia de Telecomunicaciones ha encontrado en el desarrollo de este sistema una idea innovadora que le permite satisfacer sus necesidades y proyectarse a futuras mejoras. Luego de evaluar los resultados obtenidos, la SUPERTEL ha iniciado un nuevo proyecto para expandir el alcance del sistema ASTEM.

El proyecto de la SUPERTEL, denominado Sistema Avanzado de Control de Tráfico Internacional basado en ASTERISK (SATiX), está basado en las ideas recogidas en este trabajo, y desarrolla un sistema similar para realizar pruebas de lazo cerrado. Como una de las principales mejoras, el proyecto SATiX implementará un servidor con 48 líneas telefónicas, y aplicaciones cliente en las distintas regionales de la SUPERTEL en el Ecuador.

En el nuevo alcance se busca incluir a las intendencias y delegaciones de la SUPERTEL en el Ecuador en las pruebas de lazo cerrado. Para esto, las aplicaciones cliente en el sistema SATiX también permitirán conectar líneas telefónicas para realizar pruebas de lazo cerrado, sin embargo en estas aplicaciones cliente únicamente se podrán recibir llamadas. Las pruebas de lazo cerrado que se realicen podrán terminar o no en el sistema. Para evaluar los resultados de las llamadas que no terminen en el sistema, este permitirá ingresar un archivo con los CDR de la operadora para que sean comparados con los CDR del sistema.

El sistema también integrará módulos para iniciar llamadas de lazo utilizando software de telefonía vía Internet como Skype, Google Talk, o Yahoo talk; portales de compra y venta de minutos de telefonía; y, proveedores de telefonía internacional en la bolsa de tráfico.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

5.1.1 CONCLUSIONES TECNOLÓGICAS

1. La telefonía tradicional está siendo desplazada por la Voz sobre IP. Este nuevo método para realizar llamadas permite abaratar costos en las llamadas sin sacrificar calidad, lo cual la hace muy atractiva. En la actualidad existen varios protocolos desarrollados para esta tecnología, como SIP o IAX, los cuales se han vuelto más populares con el paso del tiempo dado su buen desempeño.

2. Las PBX's basadas en software libre son una respuesta completa y accesible para la telefonía de empresas y negocios. Estas PBX's se basan en sistemas operativos LINUX, por lo general, y permiten integrar servicios de telefonía de manera sencilla y económica. Además, soluciones como ASTERISK son muy flexibles y pueden ser configuradas de acuerdo a las

necesidades del cliente para cumplir funciones específicas en telefonía, como llamadas automáticas.

3. Los fraudes en telecomunicaciones tienen la característica de adaptarse a los avances tecnológicos. Nuevos desarrollos permiten a los defraudadores ingeniarse nuevas formas de cometer estos delitos. Por ejemplo, el tipo de sistemas “bypass” que se implementaban hace unos años es completamente diferente a los que se implementan hoy, ya que ahora es posible acceder a enlaces de internet y equipos de telecomunicaciones o redes con mucha facilidad.

4. Entre los tipos de fraudes en telecomunicaciones que no involucran un conocimiento técnico, resaltan los fraudes por roaming, robo de líneas, y fraude por suscripción. Este tipo de fraudes están relacionados con la forma en que el defraudador adquiere el servicio, ya que proporcionando datos falsos, o apoderándose de una línea asignada a otro persona, éste pretende no pagar los consumos realizados.

5. Existen diferentes métodos para combatir el fraude de sistemas telefónicos “bypass”. Algunos de éstos son preventivos y otros proactivos. Hoy en día, este tipo de fraudes ha concentrado esfuerzos en la telefonía celular ya que ésta, por su carácter inalámbrico, dificulta la tarea de ubicación física de la instalación clandestina. Además, las PBX's implementadas con software libre se presentan como una alternativa económica para cursar tráfico no autorizado.

6. El proceso de detección y neutralización de sistemas telefónicos “bypass” comienza por la identificación de las líneas y su ubicación geográfica. Se han desarrollado dos técnicas para identificar líneas telefónicas utilizadas en sistemas “bypass”. La primera, denominada lazo cerrado, se basa en la realización de llamadas para identificar la ruta a través de la cual el tráfico telefónico ingresa. La segunda, denominada perfilamiento telefónico, realiza un análisis de la cantidad de tráfico cursado por las líneas telefónicas, y filtra aquellas líneas que presentan cantidades de tráfico inusual.

7. La ubicación geográfica de un sistema de telefonía no autorizado depende del tipo de telefonía que se utilice. Para la ubicación en telefonía fija se utilizan los registros de instalación de las líneas. Cuando se trata de líneas de telefonía móvil, se utilizan métodos de triangulación.

8. En el Ecuador, los sistemas telefónicos no autorizados han aumentado en los últimos años. Los principales proveedores afectados han sido los de telefonía celular y CNT en el caso de telefonía fija. Este tipo de sistemas se han visto beneficiados por el fácil acceso a Internet y equipos de red que permiten implementar sistemas telefónicos de manera relativamente sencilla.

9. Se puede observar que la cantidad de llamadas internacionales, y por ende, la cantidad de tráfico desde y hacia el Ecuador ha bajado en los últimos años; sin embargo, esto no implica necesariamente un aumento o disminución de la cantidad de sistemas telefónicos no autorizados.

10. La cantidad de tráfico telefónico internacional entrante al Ecuador es mucho mayor a la de tráfico saliente. Este fenómeno se puede atribuir a las facilidades que existen en el extranjero para realizar llamadas hacia Ecuador, como tarjetas de telefonía pre-pagada, portales WEB, etc.; y, al costo que las operadoras cobran por una llamada internacional realizada desde Ecuador.

11. Las llamadas de lazo cerrado deben ser realizadas aleatoriamente durante el transcurso del año y con especial énfasis durante días festivos, donde el volumen de tráfico telefónico internacional es mayor. Como se observó en el análisis estadístico, para obtener resultados confiables es necesario dividir el año en partes para realizar varios grupos de pruebas y, dado el alto número de llamadas, el número de pruebas por grupo debe ser al menos 385.

12. El mercado de las telecomunicaciones mundial utiliza indicadores para determinar calidad, tiempos de conexión, e incluso costos de las llamadas. La mayoría de estos indicadores están estandarizados por la UIT y permiten evaluar el rendimiento de una red telefónica internacional.

13. Una de las alternativas para la telefonía internacional son los portales de compra y venta de minutos. Aquí se negocia tráfico telefónico internacional hacia países en todo el mundo. Estos portales son una opción para que empresas creen enlaces telefónicos directos entre sus sucursales; sin embargo, pueden ser utilizados para cometer fraude telefónico tipo “bypass”.

14. Las regulaciones con las que el Ecuador cuenta en el campo de las telecomunicaciones necesitan una actualización dado el progreso que este sector ha tenido en los últimos años. Es necesario que la ley contemple situaciones reales y sea más específica para determinar que es o no un delito en telecomunicaciones, y cuáles deben ser las sanciones. Esta misma idea es aplicable al sector informático.

15. Las PBX ASTERISK ofrecen una variedad de aplicaciones en telefonía. Se ha podido observar que está diseñada en módulos, los cuales además facilitan configurarla para interactuar con aplicaciones externas. Esto permite el desarrollo de software propietario que controle y configure la central.

16. El desarrollo de un sistema debe partir de las necesidades del cliente. Es importante considerar las diferentes funcionalidades del mismo, y posibles problemas durante la implementación. Esto facilita el desarrollo del software y permite corregir errores a tiempo. Para el planteamiento de las necesidades el modelo UML utiliza los “Casos de uso”, los cuales permiten proponer una respuesta a los requerimientos del cliente. Una vez lista una posible solución para los problemas, ésta debe ser analizada con el usuario para verificar que se cumplen sus necesidades.

17. Durante el diseño de un sistema es necesario considerar posibles mejoras o adiciones futuras a fin de desarrollar una solución que satisfaga las expectativas del usuario. Este trabajo se facilita cuando el diseño de la aplicación está basado en objetos, como por ejemplo, utilizando la metodología de diseño UML.

18. Los lenguajes de programación deben estar acorde al diseño planteado al inicio de un proyecto. Sin embargo, los lenguajes de programación más comunes, como JAVA, C#, o PHP, están definidos utilizando el concepto de objetos. Además, según el software que se desee implementar, se debe escoger el lenguaje más adecuado. En este proyecto, tras un análisis de sus ventajas y desventajas, se observó que para aplicaciones que manejan múltiples hilos la mejor opción entre JAVA y PHP es JAVA.

19. Es importante considerar aspectos de seguridad al diseñar soluciones distribuidas. La seguridad es trascendental para garantizar la integridad de la información que se almacena y el correcto uso de los elementos en el sistema. Por ejemplo, la PBX ASTERISK debe contar con medidas adecuadas en configuración y acceso a Internet para evitar que sea víctima de un “fraude a PBX”.

5.1.2 CONCLUSIONES ECONÓMICAS

1. El perjuicio que este tipo de fraudes generan en el sector de las telecomunicaciones es bastante alto. Implementar esta solución le permite al estado contar con mejores herramientas para el combate a estos ilícitos, lo cual implica un ahorro por la cantidad de tráfico internacional que se evitará perder.

2. El costo de los equipos necesarios para esta solución es mucho menor al costo en soluciones similares. Esto se refleja en dos aspectos, el costo de adquisición y el costo de mantenimiento. En soluciones comerciales similares se utiliza mayor cantidad de equipos, lo cual significa mayor costo de implementación y gastos por mantenimiento. Además el sistema requiere menor espacio para ser implementado.

3. El costo total de desarrollo e implementación del sistema es menor al costo de soluciones comerciales similares, ya que estas, por ser software propietario, requieren licencias que deben ser actualizadas cada cierto periodo de tiempo que generalmente es un año. El sistema, por otro lado, no requiere licencias de funcionamiento.

4. El costo de implementar nuevas funcionalidades al sistema es bajo. Esto se debe a que el software es código abierto y propiedad de la SUPERTEL, por lo cual se puede realizar ajustes y actualizaciones sobre el software directamente. En el caso de aplicaciones comerciales implementar cambios puede incluso requerir un nuevo sistema.

5.1.3 CONCLUSIONES FUNCIONALES

1. La conexión remota que ofrece el sistema al ser una aplicación distribuida permite acceder a él desde cualquier parte, sin que este sea una página WEB disponible en Internet. La aplicación de escritorio en JAVA da al usuario un entorno amigable para interactuar con las funciones del sistema contenidas en el servidor.

2. El tipo de interfaz gráfica que la aplicación maneja a través del programa cliente facilita su uso y administración. Esta interfaz gráfica puede ser utilizada sobre cualquier sistema operativo que tenga instalada la máquina virtual de JAVA.

3. A diferencia de soluciones comerciales parecidas, el sistema desarrollado permite realizar llamadas simultáneas desde un mismo computador, y controladas a través de un solo software. Estas llamadas son manejadas de forma independiente y generan sus propios CDR.

4. La opción de programar pruebas o grupos de pruebas facilita la generación de llamadas durante noches y días festivos, sin necesidad de que un usuario se encuentre presente. Se pueden generar grupos de llamadas inmediatamente o definidos para una fecha y hora en el futuro.

5. El sistema desarrollado tiene la característica de generar CDR's de acuerdo a las especificaciones definidas por el usuario. En una aplicación comercial, los CDR están definidos en el software independientemente de las necesidades del cliente. En este caso, adicionalmente, es posible agregar información que pueda ser necesaria en el futuro.

6. La interfaz implementada para el manejo de tarjetas de telefonía pre-pagada facilita el registro y administración de éstas. Cuando se desea

ingresar una nueva tarjeta es posible utilizar datos de otras tarjetas previamente almacenadas.

7. El método de generación de alertas permite al usuario tener información en tiempo real sobre los resultados de pruebas que se están ejecutando. Cuando un número es identificado como sospechoso, el usuario recibe en una cuenta de correo electrónico un e-mail con la información principal de la llamada, y puede encontrar la información detallada del evento en la base de datos del sistema.

8. La funcionalidad que ofrece el sistema para realizar consultas a su base de datos facilita el manejo a usuarios no expertos en el tema. El usuario puede seleccionar y filtrar la información que desea analizar utilizando las opciones en la ventana de consultas. Además, permite generar informes con la información solicitada por el usuario.

9. Los registros del sistema son muy importantes para realizar un seguimiento a las actividades del mismo, y determinar la causa de cualquier error que pueda presentarse.

5.2 RECOMENDACIONES

1. Al implementar una PBX, sea ésta para utilizarse como central telefónica o alguna aplicación diferente, se debe considerar los diferentes tipos de protocolos, como SIP, IAX, H323, y la compatibilidad entre los equipos. Para conectar dos PBX ASTERISK es recomendable utilizar IAX por la compatibilidad que tienen, sin embargo SIP tiene mayor acogida y muchos fabricantes incluyen en sus equipos soporte para este protocolo.

2. Para implementar una PBX ASTERISK se debe tener en cuenta que se es una víctima potencial de “fraude de PBX”. Es recomendable comprobar que la configuración limita el acceso a los usuarios para realizar llamadas internacionales, y no acepta usuarios anónimos. Además, es útil evitar utilizar conexiones directas a través de Internet.

3. El sistema desarrollado puede ser implementado utilizando Gateways telefónicos, sin embargo, estos presentan una serie de problemas de configuración que limitan las funcionalidades del sistema. Es preferible utilizar tarjetas de telefonía analógica, las cuales tienen mejor compatibilidad con ASTERISK.

4. En la práctica, es recomendable combinar el método de lazo cerrado con perfilamiento telefónico a fin de verificar los resultados obtenidos por las pruebas. En los números identificados por el sistema se analiza el tráfico y se los compara con otros números para determinar si el número está siendo utilizado en un “bypass”.

5. Es recomendable que la SUPERTEL coordine con las operadoras de telefonía para que estas no envíen identificadores de *Caller ID* en blanco, con números sin sentido, o con información basura, ya que esto no permite verificar la naturaleza de la ruta de una llamada.

6. Para elegir la metodología de diseño se debe analizar las circunstancias y facilidades del desarrollador. Es necesario tener en cuenta que en metodologías como la XP, el desarrollo debe estar estrechamente relacionado con el usuario, en cuyo caso muchas veces esto puede ser motivo de retraso en la consecución de la solución.

7. La investigación de fraudes en telecomunicaciones tipo “bypass” requieren herramientas integrales; por lo cual, se debe considerar agregar funciones al sistema, como el manejo de portales WEB. Además, es conveniente que el administrador enfoque sus pruebas en aquellas tarjetas de telefonía que presentan mayor cantidad de irregularidades.

8. Es recomendable que la SUPERTEL mantenga una base estadística respecto al tráfico telefónico internacional desde y hacia Ecuador. Esta información debe ser utilizada como herramienta para definir nuevas estrategias en el combate a ilícitos en telecomunicaciones, y propuestas de actualización o reforma a las leyes.

9. Los organismos legislativos deben prestar más atención a las normativas y leyes existentes en el campo de las telecomunicaciones. La situación del país requiere leyes más claras y concisas al respecto, que definan los delitos y sus sanciones, y facilite la utilización de la tecnología.

GLOSARIO

Ataque de fuerza bruta.- Es una técnica que intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Broadcast.- Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Caller ID.- Es un servicio de telefonía que transmite el número telefónico del abonado que genera una llamada durante el timbrado; este número es recibido en el equipo del usuario que recibe la llamada. Dependiendo de las zonas geográficas y de las compañías el sistema puede ser prestado en varios formatos y con diferentes informaciones. En ciertas ocasiones, el término es utilizado para referirse al número del abonado que genera la llamada.

Carrier.- En su significado de portadora, carrier es una señal o pulso transmitido a través de una línea de telecomunicación. Un carrier es también una empresa que opera en el sector de las telecomunicaciones ofreciendo servicios de troncales telefónicas.

CDR.- Los Registros Detallados de Llamadas, o CDR por sus siglas en inglés (*Call Detail Record*), son registros sobre las llamadas realizadas y recibidas. Estos reportes contienen información como el número de llamadas realizadas, la duración de las llamadas, el origen y destino de las llamadas y el gasto de las mismas.

Dirección IP.- Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un dispositivo dentro de una red que utilice el protocolo TCP/IP. Corresponde al nivel de red del protocolo TCP/IP.

Framework.- Es una estructura conceptual y tecnológica de soporte definida, normalmente con módulos de software concretos, con base en la cual otro proyecto de software puede ser organizado y desarrollado.

Gateway.- Denominado “Puerta de enlace” en español, es un dispositivo que permite interconectar a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

GNU GPL.- La Licencia Pública General de GNU, o GNU GPL por sus siglas en inglés (*GNU General Public License*), es un tipo de licencia creada por la *Free Software Foundation* orientada principalmente a proteger la libre distribución, modificación y uso de software. Su propósito es declarar que el software cubierto por esta licencia es software libre y se prohíbe cualquier apropiación que restrinjan esas libertades a los usuarios.

H.323.- Es una recomendación de la Unión Internacional de Telecomunicaciones (ITU) que define los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red.

Hipertexto.- es un sistema para escribir y mostrar texto que enlaza a información adicional sobre ese texto. El término fue acuñado por Ted Nelson para referir a un sistema no lineal de buscar y conseguir información basado en enlaces asociativos entre documentos.

HTML.- El Lenguaje de Marcado de Hipertexto, o HTML por sus siglas en inglés (*HyperText Markup Language)*, es un lenguaje usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de «etiquetas», rodeadas por corchetes angulares (<,>).

IETF.- El Grupo Especial sobre Ingeniería de Internet, o IETF por sus siglas en inglés (*Internet Engineering Task Force*), es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, direccionamiento y seguridad.

Instancia.- Es el producto de la creación de un objeto perteneciente a una clase (se dice que el objeto es una instancia de la clase). El objeto que se crea tiene los atributos, propiedades y métodos de la clase a la que pertenece.

Java FX.- Es una familia de productos de *Sun Microsystems*, adquirida por *Oracle Corporation*, para la creación de aplicaciones web que tienen las características y capacidades de aplicaciones de escritorio, incluyendo aplicaciones multimedia interactivas.

Java ME.- *Java Micro Edition* es una especificación de un subconjunto de la plataforma Java orientada a proveer una colección certificada de APIs de desarrollo de software para dispositivos como PDAs, teléfonos móviles o electrodomésticos.

Java.- Es un lenguaje de programación orientado a objetos, desarrollado por *Sun Microsystems*. El lenguaje en sí mismo toma mucha de su sintaxis de C y C++, pero tiene un modelo de objetos más simple y elimina herramientas de bajo nivel.

Javascript.- Es un lenguaje de programación que se puede utilizar para construir sitios Web y para hacerlos más interactivos. El lenguaje *Javascript* puede interactuar con el código HTML, permitiendo a los programadores web utilizar contenido dinámico que se ejecuta del lado del cliente.

Llamadas off-net.- Son aquellas llamadas que se inician en un operador y terminan en la red de otro operador.

Llamadas on-net.- Son aquellas llamadas que terminan en la red propia del operador.

Máquina Virtual Java.- Es un máquina virtual de proceso nativo, es decir, ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en el código generado por el compilador de Java.

Multicast.- Es el envío de la información en una red a múltiples destinos simultáneamente.

Portadora.- Es una forma de onda, generalmente sinusoidal, que es modulada por una señal que se quiere transmitir. La frecuencia de esta onda es mucho más alta que la de la señal que contiene la información a transmitir.

Prompt.- Es un carácter o conjunto de caracteres que se muestran en una línea de comandos para indicar que está a la espera de órdenes.

Profiling.- Término utilizado para referirse a la técnica de perfilamiento telefónico.

PSTN.- La Red Telefónica Pública Conmutada, o PSTN por sus siglas en inglés (*Public Switched Telephone Network*), es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada.

Puerto.- Es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir. Dicha interfaz puede ser de tipo físico, o puede ser a nivel de software.

Puerto PCI.- Un puerto de Interconexión de Componentes Periféricos, o puerto PCI por sus siglas en inglés (*Peripheral Component Interconnect*), consiste en un bus de ordenador estándar para conectar dispositivos periféricos directamente a su placa base. Estos dispositivos pueden ser circuitos integrados ajustados en ésta o tarjetas de expansión que se ajustan en conectores.

Radiogoniometría.- Es la técnica utilizada para determinar el lugar del que procede una señal de radio. Las aplicaciones de esta técnica son muy extensas

Roaming.- Es la capacidad de cambiar de un área de cobertura en una red inalámbrica a otra, sin interrupción en el servicio o pérdida en conectividad. Permite a los usuarios seguir utilizando sus servicios de red inalámbrica cuando viajan fuera de la zona geográfica en la que contrataron el servicio. Por ejemplo, permite a los usuarios de teléfonos móviles de un país seguir utilizando su servicio telefónico cuando viajan a otro país.

Servlet.- Es una clase del lenguaje de programación Java utilizada para aumentar el potencial de servidores que alojan y dan acceso a aplicaciones a través del modelo de programación solicitud-respuesta. Los servlets son utilizados principalmente para extender las funcionalidades de servidores WEB.

Smartphone.- También conocido como Teléfono Inteligente, es un teléfono móvil que ofrece más funciones que un teléfono celular común. Casi todos los teléfonos inteligentes son móviles que soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal. Además

permiten la instalación de programas para incrementar el procesamiento de datos y la conectividad.

Socket.- Es una dirección que combina una dirección IP y un número de puerto.

SS7.- El Sistema de Señalización número 7 o SS7 por sus siglas en inglés (*Signaling System #7*), es un conjunto de protocolos de señalización telefónica empleado en la mayor parte de redes telefónicas mundiales. Su principal propósito es el establecimiento y finalización de llamadas.

Switch.- Los *switch* son dispositivos que filtran y encaminan paquetes de datos entre segmentos de redes locales. Operan en la capa de enlace del modelo OSI.

TCP.- El Protocolo de Control de Transmisión, o TCP por sus siglas en inglés (*Transmission Control Protocol*), es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte, actualmente documentado por IETF en el RFC 793. Es un protocolo de capa 4 según el modelo OSI.

TCP/IP.- El Protocolo de Control de Transmisión/Protocolo de Internet, o TCP/IP por sus siglas en inglés (*Transmission Control Protocol/Internet Protocol*), es un modelo de descripción de protocolos de red creado en la década de 1970. TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que una computadora pueda comunicarse en una red.

TDM.- La Multiplexación por División de Tiempo, o TDM por sus siglas en inglés (*Time-Division Multiplexing*), es una técnica que permite la transmisión de señales digitales y cuya idea es aprovechar el tiempo que existe entre paquetes de una fuente para enviar por el mismo canal paquetes de otras fuentes.

UIT.- La Unión Internacional de Telecomunicaciones, o UIT, es el organismo especializado de la Organización de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Unicast.- Es el envío de información desde un único emisor a un único receptor.

WEB.- Es un sistema de distribución de información basado en hipertexto y accesibles a través de Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, videos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

WiMAX.- La Interoperabilidad Mundial para Acceso por Microondas, o WiMAX por sus siglas en inglés (*Worldwide Interoperability for Microwave Access*), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 GHz. Es una tecnología dentro de última milla, también conocidas como bucle local, que permite la recepción de datos por microondas y retransmisión por ondas de radio. El protocolo que caracteriza esta tecnología es el IEEE 802.16.

BIBLIOGRAFÍA

Libros y artículos

[1] ALARCON, Raúl. *Diseño orientado a objetos con UML*. Primera edición, Grupo EIDOS, España, 2000.

[2] ARBINET. *Folleto de ventas y servicios*, Estados Unidos, 2010.

[3] BASET, Salman A.; SCHULZRINNE, Henning; Department of Computer Science. *An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol*, Universidad de Columbia, New York, 2004.

[4] CABEZA GALAN, Antonio. *Fundamentos básicos de las telecomunicaciones*, 1ra edición, Madrid, 2000.

[5] CAMACHO RODRÍGUEZ, Jesús, La telefonía IP en miniordenadores, Proyecto de fin de carrera, UNIVERSIDAD DE ALERÍA, 2009.

[6] CRIOLLO ROMÁN, Christian Mauricio, “El bypass en redes telefónicas celulares. Técnicas de detección de números celulares implicados y de infraestructuras ilegales”, Proyecto de Titulación, Escuela politécnica Nacional, Quito, 2008.

[7] FERNANDEZ, Luis; HERNANDEZ, Daniel. *Plataforma para servicios de valor agregado basados en localización, en una red GSM, a partir de la medición de la intensidad de señal (Parte I)*, Volumen 20, Número 3, Venezuela, 2005.

[8] GOSLING, James; JOY, Bill; STEELE, Guy; BRACHA, Gilad. *The Java Lenguaje Specification*, Tercera Edición, Addison-Wesley, Estados Unidos, 2005.

[9] HURTADO GIL, Sandra Victoria. *Representación de la arquitectura de software usando UML*, Universidad Icesi-I2T, 1999.

[10] ING. MEZA, María José. *Fraude en telecomunicaciones*, 1ra edición, editorial Publi Asesores, Quito, 2008.

[11] LANDÍVAR, Edgar. *Comunicaciones Unificadas con Elastix*, segunda edición, volumen 1 y 2, 2009.

[12] Ley Reformatoria al Código Penal No. 99-38. Reforma al artículo 422, publicada en el Registro Oficial No. 253 del 12 de agosto de 1999.

[13] MACIÁ-FERNÁNDEZ, Gabriel. Taller IIRSA / CITEL "Servicios de roaming internacional"*, El fraude en roaming: estrategias de ataque y de defensa*, Madrid, 2008.

[14] MALIK, Om. Artículo GIGAOM NETWORK: VoIP, *Not Just For Cheap Calls*, 2006.

[15] Oferta presentada a la Superintendencia de Telecomunicaciones, SISPRIN, SUPERTEL, Quito, 2007.

[16] PRESSMAN, Roger S. *Ingeniería del Software*, Quinta edición, McGraw-Hill, España, 2002.

[17] SERIE E. *Magnitudes comparativas para la gestión de la calidad de funcionamiento de las redes*, Recomendación UIT-T E.437.

[18] STALLINGS, William. *Comunicaciones y redes de computadores*, 6ta edición, Editorial Prentice – Hall, Madrid, 2003.

[19] SUPERINTENDENCIA DE TELECOMUNICACIONES. Oficio DIE-2011-00059, *Atender pedido de información relacionado con servicios de telefonía*, Quito, 2011.

[20] SUPERINTENDENCIA DE TELECOMUNICACIONES. Oficio IET-2011-00022, *Pedido de información relacionado con servicios de telefonía internacional no autorizado*, Quito, 2011.

[21] SUPERTEL; CNT; DIRECT TV. *Taller internacional de delitos en telefonía y televisión por suscripción*, Hotel DannCarlton, Quito, 2010.

[22] TANENBAUM, Andrew S. *Redes de computadoras*, 4ta edición, Editorial Pearson Educación, México, 2003.

[23] TELEFÓNICA DE ARGENTINA SA, Gerencia de Prevención y Control del Fraude. *Prevención y Control del Fraude en las Telecomunicaciones*, Argentina, 2009.

[24] UDLAP; GARDUÑO AGUILAR, Fabiola. *Software para dimensionamiento de troncales para redes*, Proyecto de titulación, México, 2007.

[25] UIT-D, Comisión de Estudio 2, Cuestión 16/2. *Manual "Sobre ingeniería de teletráfico"*, Ginebra, 2002.

[26] WALPOLE, Ronald E.; MYERS, Raymond H. *Probability & Statistics for Engineers & Scientists*, Octava edición, Prentice Hall, Estados Unidos, 2007.

Páginas WEB

[27] 2GOTEL, Wholesale. http://www.2gotel.net/wholesale.html. Acceso: 27/09/2010.

[28] 3CX, ¿Qué es un sistema telefónico PBX? http://www.3cx.es/voip-sip/sistema-telefonico-pbx.php. Acceso: 03/05/2011.

[29] ARBINET, Company Overview. http://www.arbinet.com/page.php?cid=1|13. Acceso: 06/09/2010.

[30] ASTERISK, About The Asterisk Project. http://www.asterisk.org/asterisk. Acceso: 06/05/2011.

[31] ASTERISKGUIDE, El protocolo IAX. http://www.asteriskguide.com/mediawiki/index.php/El_Protocolo_IAX. Acceso: 22/04/2011.

[32] CONATEL, Estadísticas. http://www.conatel.gob.ec/. Acceso: 02/06/2011.

[33] Directinterconect.com, About DI. http://www.directinterconnect.com/home.php. Acceso: 27/09/2010.

[34] ELASTIX, ELASTIX Overview. http://www.elastix.org/en/product-information. Acceso: 17/05/2011.

[35] EUROPEAN REGULATORS GROUP, ERG common position on VoIP. http://www.cmt.es/es/publicaciones/anexos/ERG(07)_56rev2_cp_voip_final.pdf. Acceso: 10/02/2011.

[36] EXCILA TELECOM, About Excila Telecom. http://www.excila.com/about_excila.shtml. Acceso: 24/09/2010.

[37] EXTREME PROGRAMMING, http://www.extremeprogramming.org/. Acceso: 27/01/2011.

[38] FCC, Información al consumidor. http://www.fcc.gov/cgb/spanishlinks.html. Acceso: 03/05/2011.

[39] FEDERAL COMMUNICATIONS COMMISSION; Voice Over Internet Protocol. http://www.fcc.gov/voip/. Acceso: 10/05/2011.

[40] FREEPBX, Main. http://www.freepbx.org/. Acceso: 17/05/2011.

[41] FREESWITCH, Welcome To FreeSWITCH. http://www.freeswitch.org/node. Acceso: 17/05/2011.

[42] GNU TELEPHONY, GNU Bayonne. http://www.gnutelephony.org/index.php/GNU_Bayonne. Acceso: 08/02/2011.

[43] IPSMARX, Wholesale services. http://ipsmarx.com/english/carrier/new/wholesale.html. 22/09/2010. Acceso: 27/09/2010.

[44] IPTel, VoIP no es telefonía IP. http://www.uberbin.net/archivos/rants/voip-no-es-telefonia-ip.php. Acceso: 22/11/2010.

[45] JAVA, Conozca más sobre la tecnología JAVA. http://www.java.com/es/about/. Acceso: 13/01/2011.

[46] MARKER Graciela, Informática-Hoy. http://www.informatica-hoy.com.ar/soluciones-moviles/Localizacion-de-telefonos-celulares-por-GSM-y-GPS.php. Acceso: 16/03/2011.

[47] MICROSOFT TECHNET, "Telefonía PSTN".http://technet.microsoft.com/es-es/library/cc737738(WS.10).aspx. Acceso: 27/09/2010.

[48] MINUTETRADERS, Home. http://www.minutetraders.com/. Acceso: 14/09/2010.

[49] NASER INGENIERÍA, Introducción a la Telefonía. http://www.naser.cl/sitio/Down_Papers/Introduccion%20a%20la%20telefonia.pdf. Acceso: 15/10/2010.

[50] Network Working Group, SIP: Session Initiation Protocol. http://www.ietf.org/rfc/rfc3261.txt. Acceso: 12/01/2011.

[51] Parkinson, Richard. "Traffic Engineering Techniques in Telecomunications", http://www.tarrani.net/mike/docs/TrafficEngineering.pdf. Acceso: 12/01/2011.

[52] PHP, ¿Qué es PHP? http://www.php.net/manual/es/introduction.php. Acceso: 12/01/2011.

[53] RECURSOS VoIP, Introducción. http://www.recursosvoip.com/intro/index.php. Acceso: 21/01/2011.

[54] ROMERO Pablo, Diario El Navegante. http://www.elmundo.es/navegante/2004/04/05/esociedad/1081180111.html. Acceso: 22/10/2010.

[55] SIP B2BUA, Wiki. http://www.b2bua.org/wiki/B2BUADocumentation. Acceso: 27/01/2011.

[56] SIPFOUNDRY SIPXECS IP PBX, Main page. http://sipx-wiki.calivia.com/. Acceso: 15/10/2010.

[57] STALLINGS, William, The Session Initiation Protocol. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-1/sip.html. Acceso: 22/11/2010.

[58] TELEFONÍA VOZ IP, Telefonía IP vs Telefonía Convencional. http://www.telefoniavozip.com/voip/telefonia-ip-vs-telefonia-convencional.htm. Acceso: 27/09/2010.

[59] TERACOM TRAINING INSTITUTE, “Public Switched Telephonic Network”.http://www.telecommunications-tutorials.com/tutorial-PSTN.htm. Acceso: 27/09/2010.

[60] TERRASIP, Carrier-to-carrier. http://www.terrasip.com/index.php?seite=carrier_reg&language=en&t_country=gb. Acceso: 27/09/2010.

[61] THE WORLD OF IP, ASTERISK AND LINUX. What is a gray route. http://ilovetovoip.com/2010/07/what-is-a-gray-route/. Acceso: 27/09/2010.

[62] TRIXBOX, Home. http://fonality.com/trixbox/. Acceso: 15/02/2011.

[63] UIT, Tendencias y evolución del entorno de las telecomunicaciones. https://www.itu.int/aboutitu/strategic_plans/99-03/trends-es.html. Acceso 22/09/2010.

[64] UNIVERSIDAD AUTÓNOMA DE MÉXICO, Recomendaciones para dimensionar un Sistema Asterisk. http://www.voip.unam.mx/mediawiki/index.php?title=Recomendaciones_para_dimensionar_un_Sistema_Asterisk&printable=yes. Acceso: 12/05/2011.

[65] UNIVERSIDAD AUTÓNOMA DE MÉXICO, Resumen del protocolo SIP. http://www.voip.unam.mx/archivos/docs/SIP_intro_05012008.pdf. Acceso: 27/04/2011.

[66] UNIVERSIDAD DE CASTILLA-LA MANCHA, Ingeniería Técnica de Informática de Sistemas y Gestión, Diseño y Programación Orientado a Objetos. http://www.info-ab.uclm.es/asignaturas/42579/pdf/01-Capitulo1.pdf. Acceso: 22/04/2011.

[67] UNIVERSIDAD DE CHILE, Dirección de Servicios de tecnologías de Información. http://www.telefoniaip.uchile.cl/capacitacion_telefonia.htm. Acceso: 20/04/2011.

[68] UNIVERSIDAD DE JAEN; RUEDA RUIZ, Antonio J., Programación Avanzada, Tema 4 Programación orientada a componentes. http://wwwdi.ujaen.es/asignaturas/progav/. Acceso: 21/04/2011.

[69] VOICESYSTEMONE, Qué es DID? http://www.voicesystemone.com/web/modules/xoopsfaq/index.php?cat_id=1. Acceso: 12/11/2010.

[70] VoIP FORO, Protocolos VoIP. http://www.voipforo.com/protocolosvoip.php. Acceso: 02/05/2011.

[71] VOIP MECHANIC, Basics of SIP for VoIP. http://www.voipmechanic.com/sip-call-example.htm. Acceso: 03/05/2011.

[72] VOIP.MS, Main. http://voip.ms/. Acceso: 23/09/2010.

[73] VOIP-INFO.ORG, Asterisk dimensioning. http://www.voip-info.org/wiki/view/Asterisk+dimensioning. Acceso: 12/05/2011.

[74] WIKITEL, Telefonía IP vs VoIP, http://es.wikitel.info/wiki/Telefonía_IP. Acceso: 02/12/2010.

ANEXOS

ANEXO A

GUÍA DE FUNCIONAMIENTO DEL SISTEMA

A. INTERFAZ GRÁFICA Y GUÍA DE FUNCIONAMIENTO DEL SISTEMA

La interfaz gráfica de la aplicación cliente permite a los usuarios interactuar con el servidor de manera sencilla y rápida. A través de la aplicación cliente es posible ejecutar en el servidor la mayoría de instrucciones, además de manejar los datos devueltos luego de una consulta a la base de datos.

Las funciones del sistema dan solución a los casos de uso definidos durante el diseño. A continuación una descripción de las ventanas en la interfaz gráfica, y sus funciones.

A.1. Conectar/Desconectar al servidor ASTEM

Al abrir la aplicación cliente, por defecto, esta no permite realizar ninguna acción excepto la de conectar con el servidor. Dado que el sistema se trata de una aplicación distribuida, es necesario que la aplicación cliente se conecte al servidor antes de realizar cualquier función.

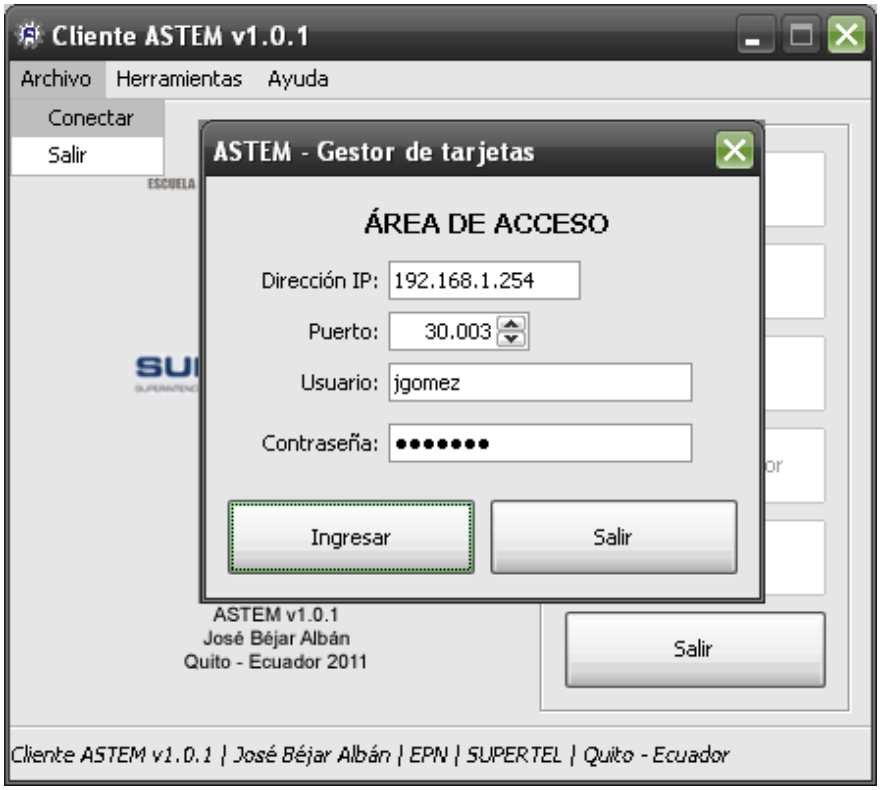


Figura A.1. Ventana de conexión del sistema ASTEM

Al iniciar la aplicación cliente, se muestra el menú principal con los botones de navegación. Estos botones se encuentran bloqueados por defecto mientras el

cliente no se encuentre conectado. Para iniciar la conexión, se deben seguir los siguientes pasos:

1. Click en el menú 'Archivo'.
2. Click en la opción 'Conectar'.
3. Se ingresan los datos del servidor.
4. Se ingresan los datos de usuario y contraseña.
5. Click en el botón 'Conectar'.

En cuanto el servidor ha recibido la solicitud y autenticado al usuario especificado, la conexión es aceptada, y se muestra un mensaje de bienvenida en la aplicación cliente. Caso contrario, se muestra un mensaje de error y el programa regresa al menú principal.

Una vez que la aplicación cliente se ha conectado exitosamente, los botones del menú principal son habilitados para permitir la navegación. El menú principal contiene las siguientes opciones:

Figura A.2. Menú principal de la aplicación cliente ASTEM

1. Menú.- Contiene las opciones del programa.
    a. Archivo.- Contiene las opciones para conectar o salir.
    b. Herramientas.- Contiene las opciones del sistema.
    c. Ayuda.- Contiene el menú de créditos.
2. Llamadas.- Accede a la ventana de generación una o varias llamadas de prueba utilizando las opciones de tarjetas, troncales y números configurados en el servidor.
    a. Generar llamada.- Genera una o varias llamadas utilizando un destino, un origen y una tarjeta de telefonía.
    b. Generar pruebas.- Genera o programa la ejecución de un grupo de llamadas de prueba.
3. Tarjetas.- Permite modificar, agregar, o eliminar los registros de tarjetas de la base de datos del servidor.
4. Registros.- Ingresa a la ventana de consultas del sistema. Permite realizar consultas a las bases de datos, clasificar la información y generar reportes.
5. Estado del servidor.- Muestra las principales actividades que se encuentra realizando el servidor.
6. Configuración.- Permite modificar las opciones de configuración del sistema ASTEM y de la PBX ASTERISK.
    a. Configuraciónes de ASTEM.- Opciones de configuración de ASTEM.
    b. Configuraciones de ASTERISK.- Opciones de configuración de la PBX ASTERISK.
7. Salir.- Cierra la aplicación cliente.

Para finalizar el trabajo y terminar la conexión establecida con el servidor, se selecciona la opción ‘Desconectar’ en el menú ‘Archivo’. El servidor envía un

mensaje de despedida y cierra la conexión. La aplicación cliente muestra el mensaje en pantalla y bloquea las opciones del menú principal.

A.2. Realizar llamadas de prueba

El botón 'Llamada' despliega dos opciones 'Generar Llamada' y 'Generar Pruebas'. Para realizar llamadas de prueba se debe seleccionar la opción 'Generar Llamada'. Se abre la ventana de opciones de llamada donde se deben seleccionar los siguientes parámetros.

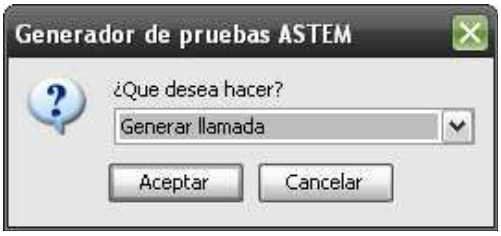


Figura A.3. Opciones del menú llamada

1. Tarjeta.- Código de la tarjeta a utilizar para realizar las llamadas prueba.
2. Teléfono.- Número de teléfono al que se dirigirá la llamada de prueba.
3. Troncal.- Troncal que se utilizará para realizar la llamada.
4. Cantidad.- Número de llamadas a realizar.

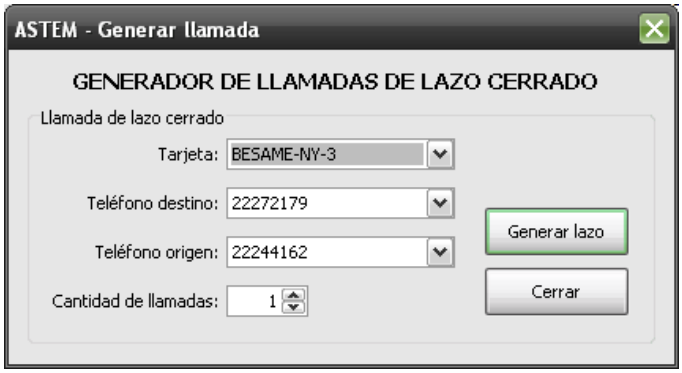


Figura A.4. Generador de llamadas de lazo cerrado

Una vez especificados estos parámetros se selecciona la opción 'Generar lazo' para iniciar las llamadas de prueba. Una vez que el servidor haya procesado la instrucción, se muestra un mensaje de confirmación.

La opción 'Cerrar' permite cancelar la generación de llamadas.

A.3. Programar un grupo de llamadas de prueba

El botón 'Llamada' despliega dos opciones 'Generar Llamada' y 'Generar Pruebas'. Para realizar llamadas de prueba se debe seleccionar la opción 'Generar Pruebas'. Se abre la ventana de opciones de prueba donde se deben seleccionar los siguientes parámetros.

Figura A.5. Generador de grupo de pruebas de lazo cerrado

1. Ejecución.- Seleccionar el inicio de las pruebas.
    a. Fecha.- Fecha de inicio de las pruebas.
    b. Hora.- Hora de inicio de las pruebas.
2. Tarjeta.- Código de la tarjeta a utilizar para realizar las llamadas prueba.

3. Troncal.- Troncal que se utilizará para realizar la llamada.
4. Teléfono.- Número de teléfono al que se dirigirá la llamada de prueba.
    a. Cantidad.- Número de llamadas a realizar.
5. Intentos.- Número de intentos cuando no se pueda conectar con la operadora.

En esta ventana se presenta la opción 'Ejecución' en la sección calendario. En caso de seleccionar 'Inmediata', el grupo de llamadas de prueba se realiza inmediatamente después de procesar la instrucción en el servidor. Caso contrario, si se selecciona la opción 'Programada' se debe especificar una fecha y hora futura para iniciar las pruebas de lazo cerrado. Una vez que el comando sea procesado en el servidor, este esperará hasta que llegue la fecha y hora especificadas para iniciar la ejecución de las llamadas de prueba.

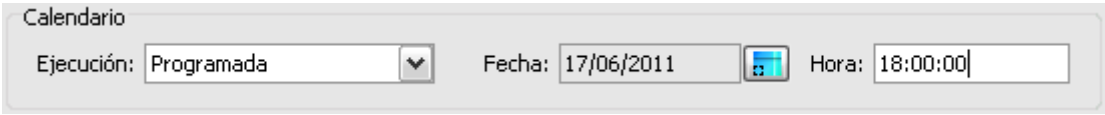


Figura A.6. Sección calendario en la ventana de generación de grupo de pruebas

Para agregar una o más tarjetas debe seleccionarlas en la lista de origen (en la sección Opciones) y dar click en el botón 'Agregar' justo debajo de la lista. El mismo procedimiento se realiza para agregar las troncales a utilizar en la prueba. Los números de teléfono deben ser agregados individualmente especificando el número de llamadas a realizar a cada número. Para esto, se selecciona un número de la lista de origen en la sección Opciones y se define un número de pruebas para el número seleccionado. Finalmente se lo agrega utilizando el botón 'Agregar'.

Para eliminar una o más tarjetas de las pruebas a realizar, se debe seleccionar las tarjetas a eliminar de la lista de tarjetas en la sección 'Pruebas a realizar' y dar click sobre el botón 'Eliminar' debajo de la lista. El mismo procedimiento se debe realizar para eliminar troncales o números telefónicos destino en las listas correspondientes.

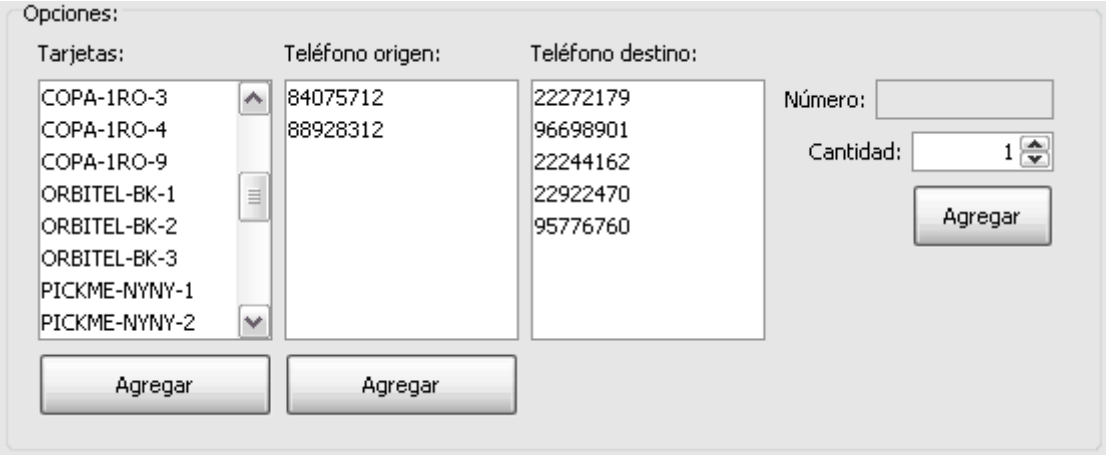


Figura A.7. Sección opciones en la ventana de generación de grupo de pruebas

Una vez especificados estos parámetros se especifica el número de intentos que la PBX debe realizar en caso de que una llamada no pueda ser conectada con la operadora (3 por defecto). Finalmente, seleccionando la opción 'Programar' se envía la instrucción para procesar el grupo de llamadas de prueba. Una vez que el servidor haya procesado la instrucción, se muestra un mensaje de confirmación.

La opción 'Cerrar' permite cancelar la generación de llamadas.

A.4. Administrar base de datos de tarjetas

A través de la opción 'Tarjetas' en el menú principal, se ingresa a la ventana de administración de tarjetas de telefonía pre-pagada. En esta ventana es posible modificar las opciones de tarjeta y agregar o eliminar una tarjeta.

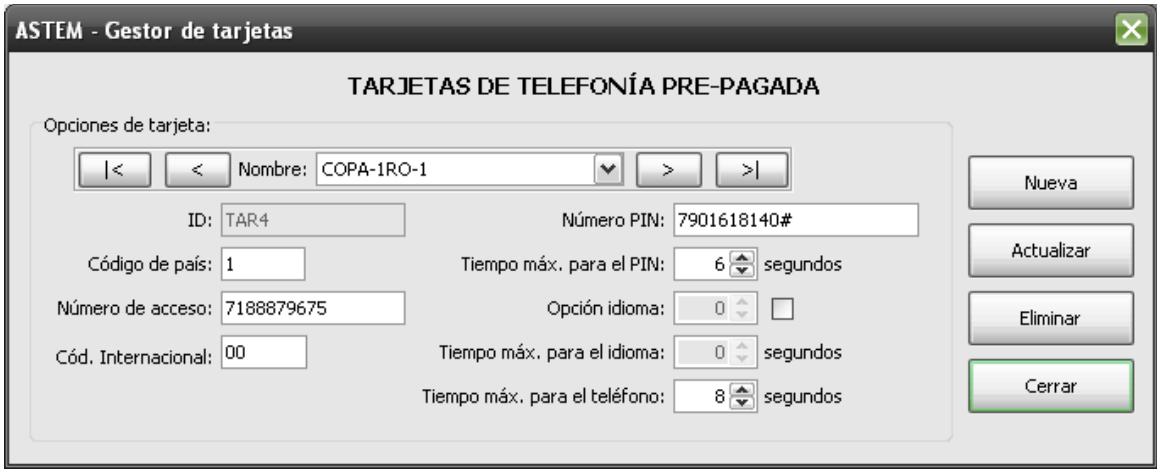


Figura A.8. Ventana del administrador de tarjetas

En la ventana de administración de tarjetas se observan los siguientes campos:

1. Opciones de tarjeta.- Contiene los datos de llamada de las tarjetas de telefonía. Estos datos son:
    a. Código de la tarjeta.
    b. Nombre de la tarjeta.
    c. Código de discado al país de la tarjeta.
    d. Número de acceso (teléfono de la operadora).
    e. Código de salida internacional en el país de la tarjeta.
    f. Número PIN.
    g. Tiempo de espera para ingresar el PIN (segundos).
    h. Activar opción de idioma.
    i. Opción de idioma.
    j. Tiempo de espera para ingresar la opción de idioma (segundos).
    k. Tiempo de espera para ingresar el teléfono destino (segundos).
2. Menú de navegación.- El menú de navegación permite seleccionar las tarjetas de la lista. Utilizando los botones se puede navegar a través de la lista hacia adelante o hacia atrás. Se puede seleccionar una tarjeta específica en la lista utilizando la lista desplegable que se encuentra entre los botones de navegación.
3. Nueva.- Permite agregar una tarjeta al sistema. Al seleccionar esta opción los campos de tarjeta quedan en blanco para ingresar los datos, y los botones ‘Nueva’ y ‘Actualizar’ toman nuevas funciones.
    a. Cancelar.- Cancela la opción de nueva tarjeta y regresa el menú al estado inicial. La opción ‘Cancelar’ se activa cuando el usuario selecciona la opción ‘Nueva’.

4. Actualizar.- Actualiza los datos de una tarjeta. Esta opción guarda los datos contenidos en las opciones de tarjeta y envía la información al servidor para que sea actualizada.

    a. Guardar.- Guarda la información de la tarjeta ingresada. La opción 'Guardar' se activa cuando el usuario selecciona la opción 'Nueva'.

5. Eliminar.- Elimina la tarjeta actual del registro del sistema. Esta opción requiere confirmación para ejecutarse.

6. Cerrar.- Al cerrar la ventana la aplicación pregunta si el usuario desea guardar los cambios de forma permanente.

Cuando la ventana de administración de tarjetas es abierta, la aplicación solicita la información de tarjetas al servidor y crea la lista para que sea mostrada. En la ventana de administración se utiliza el menú de navegación para seleccionar una tarjeta y actualizar los campos que se desee. De igual forma se puede agregar una tarjeta o eliminarla. Para eliminar una tarjeta se utilizan su código.

Al cerrar la ventana de administración, la aplicación pregunta al usuario si desea guardar los cambios de forma permanente. Si la respuesta es afirmativa, la aplicación envía una instrucción al servidor para que la información de tarjetas de telefonía sea escrita en el archivo "tarjetas.astem". Caso contrario, los cambios permanecen temporalmente mientras el servidor se ejecute.

A.5. Realizar una consulta a la base de datos

Las consultas a la base de datos se realizan a través de la opción 'Registros' en el menú principal. En la ventana de registros se puede generar consultas a la base de datos de ASTERISK y ASTEM. En la tabla de ASTERISK se puede consultar los CDR generados por la PBX, mientras que en la tabla de notificaciones se puede realizar una consulta de las alertas generadas por llamadas recibidas.

La ventana de registros se encuentra dividida con 2 pestañas. Las pestañas tienen básicamente las mismas opciones y son las siguientes:

1. Tipo de consulta.- Permite seleccionar la forma de crear la consulta. Las opciones son 'Estándar' y 'Personalizada'.

2. Lista de campos origen.- Contiene la lista de campos de la base de datos a consultar.

3. Lista de campos a consultar.- Contiene la lista de campos seleccionados para la consulta.

4. Botones de selección.- Permiten agregar o eliminar campos para realizar una consulta.

5. Condición.- Recibe una condición para la consulta.

6. Limpiar.- Limpia los campos y regresa la ventana a su estado original.

7. Consultar.- Envía la instrucción de consulta al servidor con los datos especificados.

8. Cerrar.- Cierra la ventana de registros.

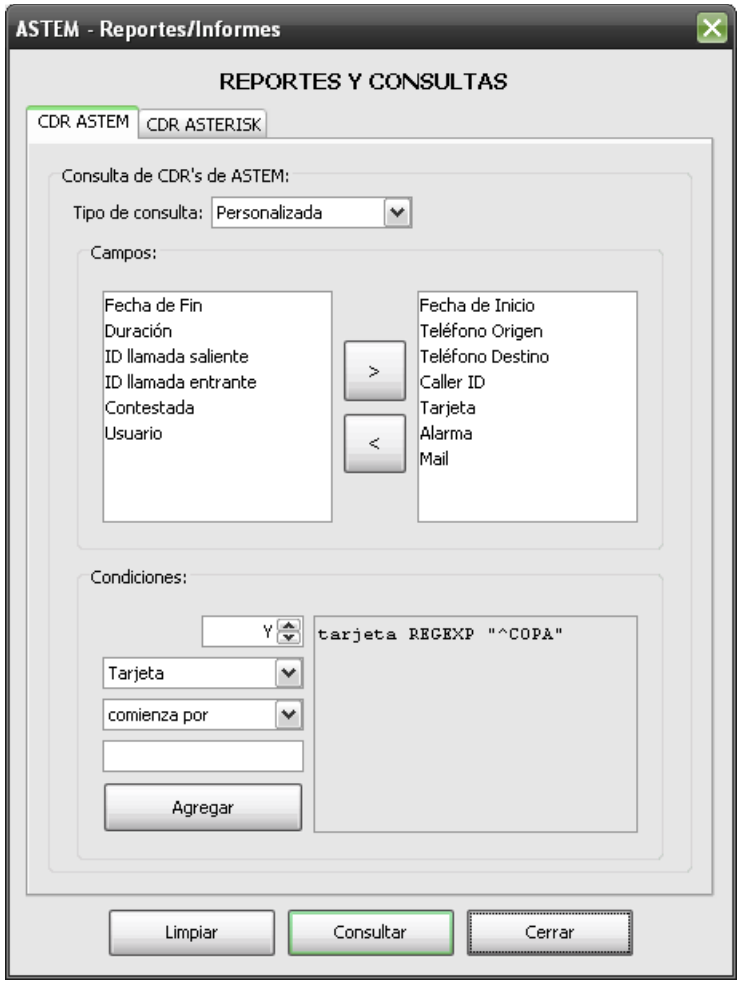


Figura A.9. Ventana de la opción 'Registros'

Una consulta tiene principalmente 3 partes, la primera donde se especifica la tabla que se desea consultar, la segunda donde se especifican los campos que se desea consultar, y la tercera donde se especifica una condición para filtrar los datos de la búsqueda.

Para realizar una consulta a la base de datos de CDR's se debe seleccionar la pestaña CDR, mientras para realizar una consulta a las alertas generadas se debe seleccionar la pestaña Notificaciones. La opción 'Estándar' construye una consulta sin condiciones con los campos "calldate", "clid", "src", "duration", y "userfield" en el caso de consultar a los CDR y "hora", "callerID", y "enviado" para una consulta de notificaciones.

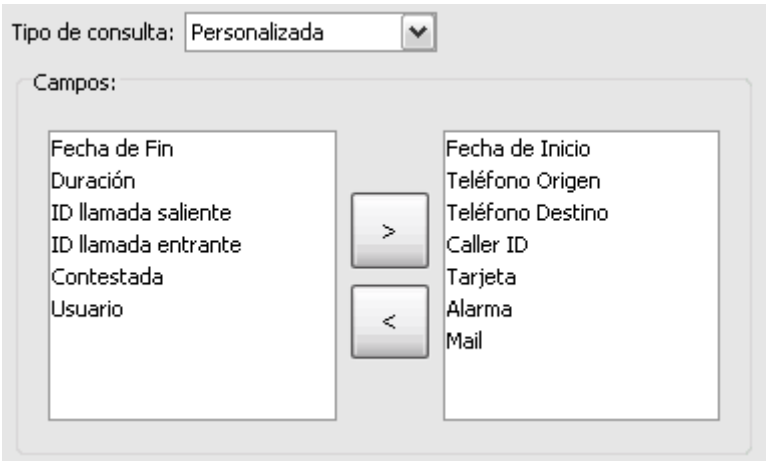


Figura A.10. Campos a seleccionar para una consulta de CDR's

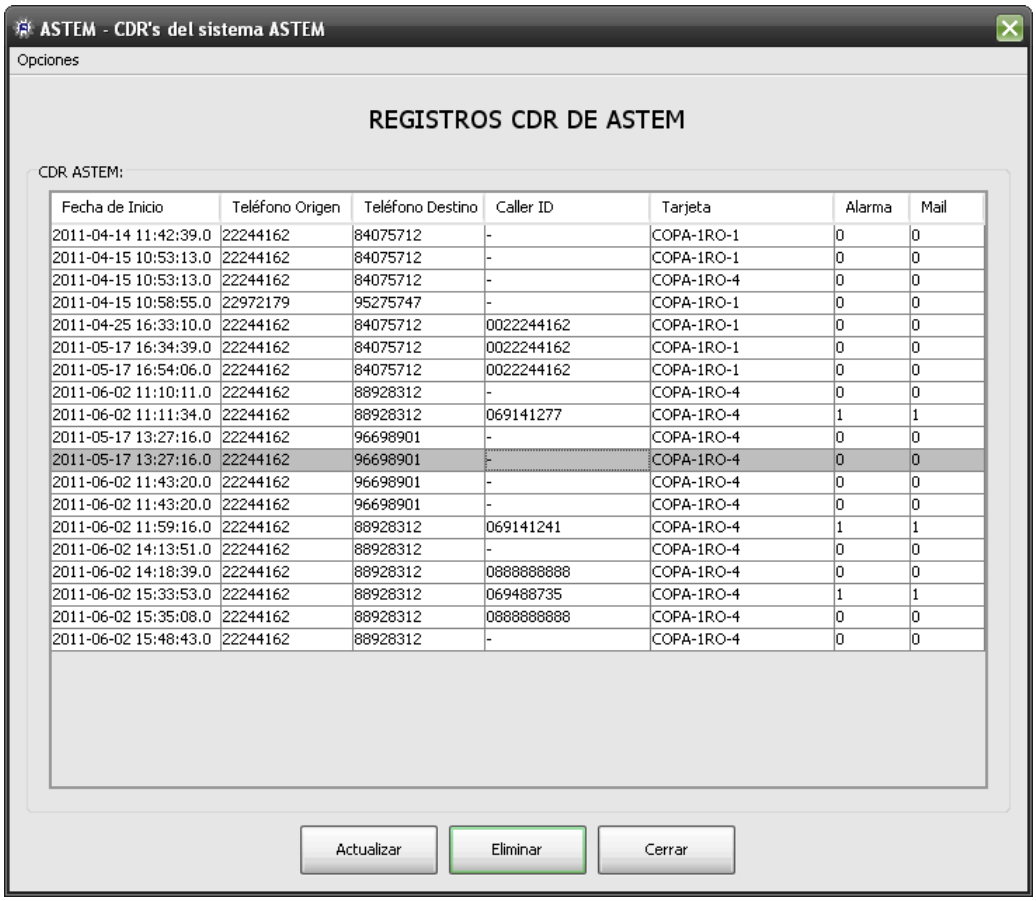
La opción 'Personalizada' permite estructurar una consulta con parámetros definidos por el usuario. Al seleccionar la opción 'Personalizada' se activan las listas de campos y el campo de texto 'Condición' para que el usuario seleccione los campos que desea consultar y defina una condición para la búsqueda. La condición debe estar en el formato de una condición MySQL y utilizando los nombres de reales de las columnas en la tabla que se consulta. Por ejemplo, una línea de condición puede ser "clid='095255747'".

Cuando una consulta ha sido estructurada, utilizando la opción 'Consultar' se envía la instrucción al servidor para que sea procesada. Una vez que el servidor procese la instrucción, la información será devuelta a la aplicación cliente.

La opción 'Cerrar' permite salir de la ventana de consultas.

A.6. Generar reportes utilizando la información de una consulta

Para generar un reporte es necesario haber realizado una consulta. Luego de procesar una consulta, la información devuelta por el servidor es mostrada en una tabla.



Fecha de Inicio	Teléfono Origen	Teléfono Destino	Caller ID	Tarjeta	Alarma	Mail
2011-04-14 11:42:39.0	22244162	84075712	-	COPA-1RO-1	0	0
2011-04-15 10:53:13.0	22244162	84075712	-	COPA-1RO-1	0	0
2011-04-15 10:53:13.0	22244162	84075712	-	COPA-1RO-4	0	0
2011-04-15 10:58:55.0	22972179	95275747	-	COPA-1RO-1	0	0
2011-04-25 16:33:10.0	22244162	84075712	0022244162	COPA-1RO-1	0	0
2011-05-17 16:34:39.0	22244162	84075712	0022244162	COPA-1RO-1	0	0
2011-05-17 16:54:06.0	22244162	84075712	0022244162	COPA-1RO-1	0	0
2011-06-02 11:10:11.0	22244162	88928312	-	COPA-1RO-4	0	0
2011-06-02 11:11:34.0	22244162	88928312	069141277	COPA-1RO-4	1	1
2011-05-17 13:27:16.0	22244162	96698901	-	COPA-1RO-4	0	0
2011-05-17 13:27:16.0	22244162	96698901	-	COPA-1RO-4	0	0
2011-06-02 11:43:20.0	22244162	96698901	-	COPA-1RO-4	0	0
2011-06-02 11:43:20.0	22244162	96698901	-	COPA-1RO-4	0	0
2011-06-02 11:59:16.0	22244162	88928312	069141241	COPA-1RO-4	1	1
2011-06-02 14:13:51.0	22244162	88928312	-	COPA-1RO-4	0	0
2011-06-02 14:18:39.0	22244162	88928312	0888888888	COPA-1RO-4	0	0
2011-06-02 15:33:53.0	22244162	88928312	069488735	COPA-1RO-4	1	1
2011-06-02 15:35:08.0	22244162	88928312	0888888888	COPA-1RO-4	0	0
2011-06-02 15:48:43.0	22244162	88928312	-	COPA-1RO-4	0	0

Figura A.11. Ventana de información de consultas

Dicha tabla puede ser modificada por el usuario. En la ventana se tienen las siguientes opciones:

1. Tabla.- Contiene la información generada por una consulta.
2. Actualizar.- Actualiza los datos de la lista con los cambios que se hayan realizado.
3. Eliminar.- Elimina una o más filas de la lista.

El menú de la ventana permite realizar las siguientes tareas:

4. Recargar tabla.- Vuelve a cargar la tabla inicial de la consulta.

5. Exportar.- Genera un documento (PDF u hoja de cálculo) con la información mostrada.

6. Salir.- Cierra la ventana de información de consultas.

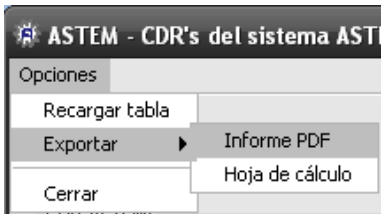


Figura A.12. Menú de creación de documentos

Una vez que la aplicación cliente recibe la información de una consulta, se abre una nueva ventana con la tabla que muestra dicha información. El usuario puede eliminar filas que no desee seleccionándolas y dando click en el botón 'Eliminar'. En caso de que requiera de nuevo la información original, es necesario hacer click en el botón 'Recargar tabla'.

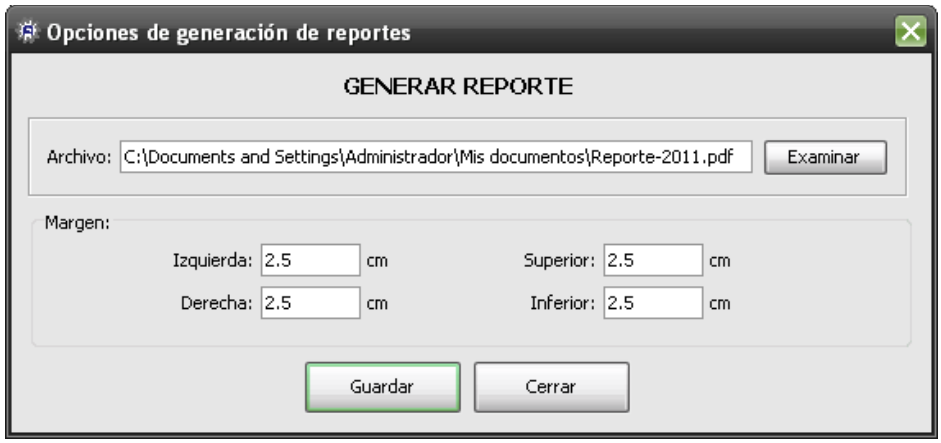


Figura A.13. Opciones de generación de consultas

La opción 'Generar reporte' permite guardar la información que se muestra en la tabla en un documento PDF. Para generar el reporte es necesario especificar el lugar donde se guardará el documento y los márgenes del mismo (por defecto son de 2.5 cm en cada lado).

A.7. Realizar una consulta estadística de las tarjetas de telefonía pre-pagada

Para realizar una consulta estadística sobre las tarjetas de telefonía se debe ingresar en el menú "Estadísticas". Se abrirá una ventana que contiene 2

pestañas. La pestana “Estadísticas” permite realizar consultas estadísticas y generar gráficos. Aquí se puede observar 4 criterios de consulta:

1. Tarjeta.- Permite seleccionar la tarjeta que se desea consultar. Si se selecciona la opción ‘Todas’, se realizará una consulta de todas las tarjetas.

2. Filtro.- Permite seleccionar el tipo de estadísticas que se desea observar. Estas pueden ser de ‘Caller ID’, ‘Tipo de llamada’ o ‘Origen’.

    a. Caller ID.- Muestra los datos de Caller ID recibidos según el tipo de tarjeta utilizada.

    b. Tipo de llamada.- Muestra el porcentaje de llamadas de lazo cerrado y llamadas de lazo abierto realizadas según cada tarjeta.

    c. Origen.- Muestra las llamadas de lazo realizadas según el número de origen y la tarjeta utilizada.

3. Inicio.- Permite definir una fecha inicial para la consulta.

4. Fin.- Permite definir una fecha final para la consulta.

Figura A.14. Ventana de consultas estadísticas de todas las tarjetas

Una vez definidos los parámetros de la consulta estadística, se selecciona la opción ‘Consultar’. Si la consulta realizada es de todas las tarjetas de telefonía pre-pagada, se mostrará un gráfico de barras con varios grupos de barras; cada grupo corresponde a una tarjeta de telefonía, como se muestra en la Figura A.14.

Si la consulta se realizó hacia una tarjeta definida, se mostrará un gráfico tipo pastel con los datos de la tarjeta. Se puede observar un ejemplo de esta consulta en la Figura A.15.

Figura A.15. Ventana de consultas estadísticas de una tarjeta

El usuario puede guardar el gráfico mostrado dando click sobre este. El gráfico se abrirá en una ventana independiente donde es posible cambiar el tamaño y seleccionar partes específicas del gráfico. Además. Dando click derecho es usuario puede guardar el gráfico como un archivo de imagen.

Adicionalmente, la ventana de estadísticas presenta la pestaña “Estado del servidor” donde se puede observar datos relacionados las pruebas realizadas. Aquí se mostrarán la cantidad de pruebas solicitadas, cantidad de pruebas de lazo cerrado, cantidad de pruebas de lazo abierto, cantidad de pruebas ejecutadas y cantidad de pruebas terminadas en el servidor desde la última vez

que se inició el servidor. Adicionalmente en esta ventana muestra si existe una cola de llamadas pendiente y es posible eliminarla con el botón 'Eliminar'. Esto eliminará la cola y no se realizarán más llamadas de prueba.

A.8. Configurar el sistema ASTEM

El botón 'Configuración' despliega dos opciones 'Configuraciones de ASTEM' y 'Configuraciones de ASTERISK'.

Para modificar las opciones del sistema ASTEM es necesario seleccionar la opción 'Configuraciones de ASTEM'.

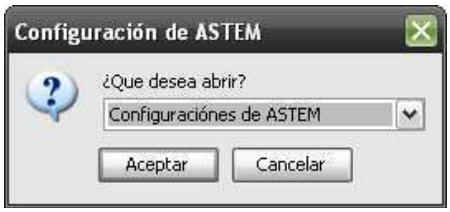


Figura A.16. Ventana de opciones de configuración

En la ventana principal de configuraciones es importante notar dos partes. En la superior se encuentra un grupo de pestañas con todas las configuraciones que afectan el funcionamiento del sistema. Estas opciones son las características de conexión, opciones de operadora, datos de conexión al monitor, datos de conexión a la base de datos, y opciones de los servidores de correo.

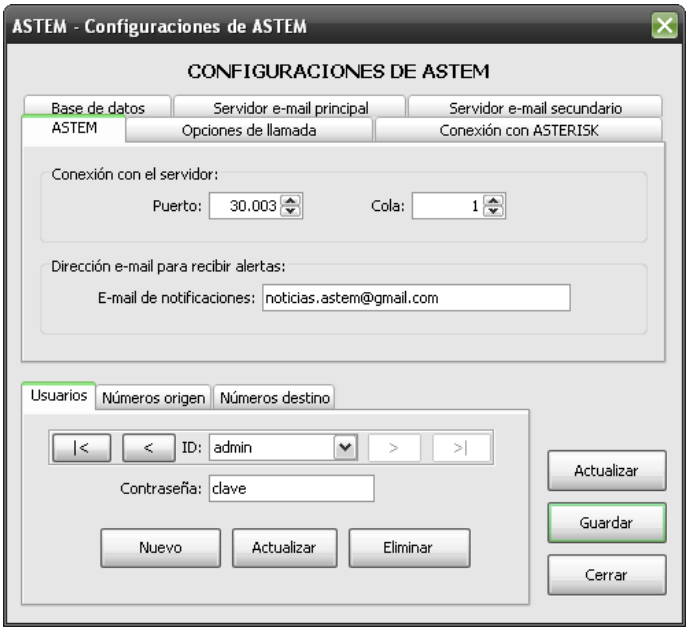


Figura A.17. Ventana de configuración del sistema ASTEM

En la parte inferior se encuentran tres pestañas que contienen la configuración de usuarios, troncales y números. Cada pestaña tiene un menú de navegación con la misma estructura que el menú de navegación del administrador de tarjetas, el cual se utiliza para seleccionar los diferentes valores en la lista.

La pestaña de usuarios permite agregar, actualizar o eliminar un usuario mientras que las pestañas de troncales y números únicamente permiten actualizar los datos. Esto se debe a que el programa está configurado para manejar únicamente 32 troncales o números.

Figura A.18. Opciones de usuarios de ASTEM

Cuando se ingresa un nuevo usuario se debe especificar el nombre y el usuario es creado con la contraseña “astem” por defecto. Una vez creado un usuario se debe cambiar la contraseña. El botón ‘Actualizar’ en estas pestañas permite guardar los cambios en el servidor y enviar la información al servidor para que sea actualizada.

Las opciones en esta ventana son

- Actualizar.- Guarda la información de la pestaña superior que se encuentra seleccionada y envía los datos al servidor para que sean actualizados.
- Guardar.- Ejecuta la instrucción para que el servidor guarde la configuración del sistema de forma permanente sobre-escribiendo los archivos “admin.astem” y “usuarios.astem” con la configuración actual.
- Cerrar.- Cierra la ventana de configuración del sistema.

A.9. Modificar la configuración de la PBX ASTERISK

El botón ‘Configuración’ despliega dos opciones ‘Configuraciones de ASTEM’ y ‘Configuraciones de ASTERISK’. Para modificar las opciones del sistema ASTEM

es necesario seleccionar la opción ‘Configuraciones de ASTERISK’ y se mostrará la ventana de la Figura A.19.

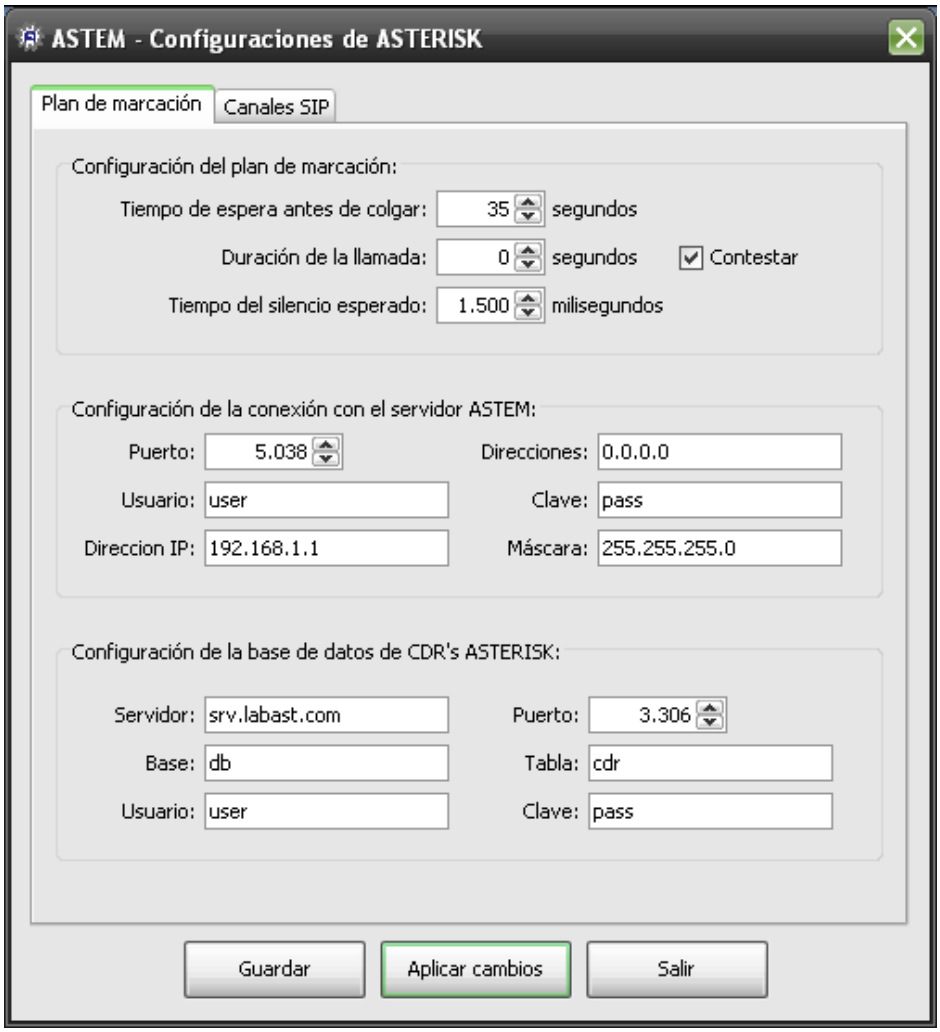


Figura A.19. Ventana de configuración de ASTERISK

El sistema ASTEM permite modificar la configuración de la PBX ASTERISK. Esta configuración se encuentra definida en los archivos y el sistema ASTEM permite modificar algunos parámetros de la configuración del monitor, la conexión de la PBX a la base de datos, los canales SIP, y el plan de marcación.

En la ventana de configuración de la PBX existen 2 pestañas y 4 opciones:

1. Pestaña General.- Contiene las configuraciones del plan de marcación, conexión al monitor y conexión a la base de datos de la PBX.
2. Pestaña Canales SIP.- Contiene la configuración SIP y los canales definidos en la PBX. Se puede agregar, modificar, o eliminar canales.

a. Editar.- Permite editar la configuración de un canal SIP.

b. Nuevo.- Agrega un nuevo canal SIP.

c. Eliminar.- Elimina un canal SIP de la configuración.

3. Guardar.- Guarda la información de la pestaña activa y la envía al servidor para que sea actualizada.

4. Aplicar cambios.- Envía la instrucción al servidor para que sobre escriba los archivos de configuración de ASTERISK con la configuración actual y reinicie el servicio.

5. Salir.- Cierra la ventana de configuración.

En la ventana de configuración se puede modificar directamente los parámetros, sin embargo para que estos surtan efecto se deben primero guardar y luego aplicar. En la pestaña de 'Canales SIP' se puede modificar las opciones de los canales utilizando el botón 'Editar'. La opción editar desbloquea las opciones del canal y permite su modificación.

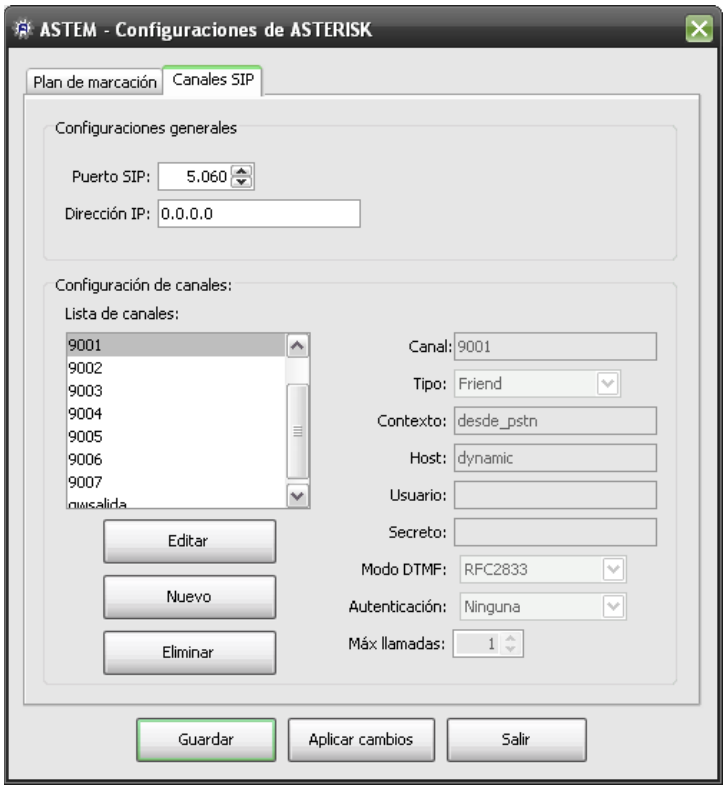


Figura A.20. Opciones de canales SIP

Cuando se ejecuta una actualización en la configuración de la PBX es necesario aplicar los cambios realizados, es decir, recargar los archivos en la PBX. Por esta razón se debe utilizar la opción 'Aplicar cambios' luego de la opción 'Guardar'. Si no se aplican los cambios, las modificaciones realizadas en la configuración de la PBX se perderán al cerrar la ventana.

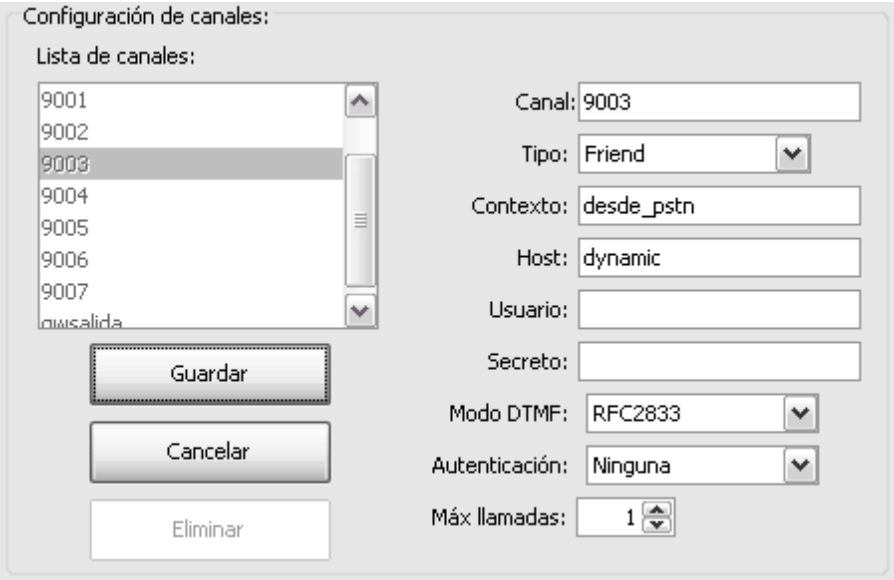


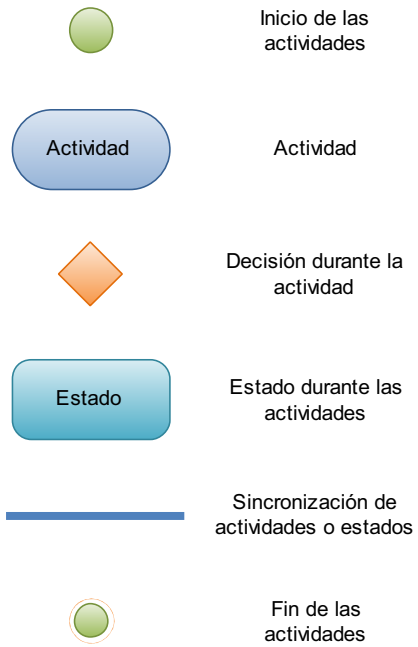
Figura A.21. Opciones de configuración de canales SIP

ANEXO B

ELEMENTOS EN UN DIAGRAMA DE ACTIVIDADES

B. ELEMENTOS EN UN DIAGRAMA DE ACTIVIDADES

Los diagramas de actividades fueron diseñados para dar una visión simplificada de lo que ocurre durante una operación o proceso. Estos diagramas son una extensión de los diagramas de estado.



B.1. Elementos en un diagrama de actividades UML

Como se observa en la Figura B.1, los diagramas de actividades incluyen los siguientes elementos:

1. *Inicio de las actividades*.- Representa el inicio de una secuencia.
2. *Actividad*.- Representa una actividad a realizarse.
3. *Decisión*.- Representa las posibles alternativas en una decisión. En toda secuencia se debe tomar decisiones en algún punto, en algunos casos las opciones de decisión pueden ser contrapuestas, es decir un “SI” y un “NO”, mientras que en otros las decisiones pueden ser actividades o estados.
4. *Estado*.- Representa un estado durante las actividades.
5. *Sincronización*.- Representa la sincronización de varias actividades o estados. Por lo general esta sincronización luego de una toma de decisión.
6. *Fin de las actividades*.- Representa el final de la secuencia.

ANEXO C

ELEMENTOS DE UN DIAGRAMA DE CLASES

C. ELEMENTOS EN UN DIAGRAMA DE CLASES

Los diagramas de clases sirven para visualizar las clases en un sistema y como estas clases se relacionan; por este motivo, un diagrama de clases está compuesto por clases y relaciones.

C.1. Clases

Este elemento representa una clase del sistema a desarrollar. Una clase está formada por atributos y métodos. En el diagrama de clases, una clase se representa con el diagrama de la Figura C.1.

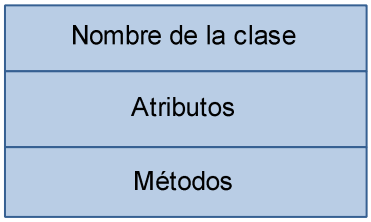


Figura C.1. Representación de una clase

En el rectángulo superior se coloca el nombre de la clase. En el rectángulo del medio la lista de atributos, y en el rectángulo inferior la lista de métodos.

C.2. Relaciones

La primera relación que existe entre clases es la cardinalidad. Esta relación define el nivel de dependencia de una clase con otra y se denota con un símbolo en cada extremo de la línea que define la relación de las clases. Los posibles símbolos son:

- *1..** .- Significa uno o muchos.
- *0..** .- Significa cero o muchos.
- *m* .- Define un número en particular.

Los diferentes tipos de relaciones entre clases son:

- Herencia.- Indica que una subclase hereda los métodos y atributos especificados por una superclase. Se representa con el símbolo de la Figura C.2.

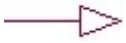


Figura C.2. Representación de herencia en un diagrama de clases

- Agregación.- Esta relación determina si el tiempo de vida de un objeto tiene relación con el tiempo de vida de otro objeto. En algunos casos un objeto existe mientras el otro exista. Se denota por el símbolo de la Figura C.3.

Figura C.3. Representación de agregación en un diagrama de clases

- Asociación.- Permite asociar objetos que colaboran entre sí. Asociación no es una relación fuerte, es decir, el tiempo de vida de un objeto no depende del otro. Se representa por el diagrama de la Figura C.4.

Figura C.4. Representación de asociación en un diagrama de clases

- Uso o dependencia.- Representa un tipo de relación muy particular, en la que una clase es instanciada. Se denota por una flecha punteada como en la Figura C.5.

Figura C.5. Representación de uso en un diagrama de clases

ANEXO D

PRUEBA DE CONSUMO DE RECURSOS DE ASTERISK

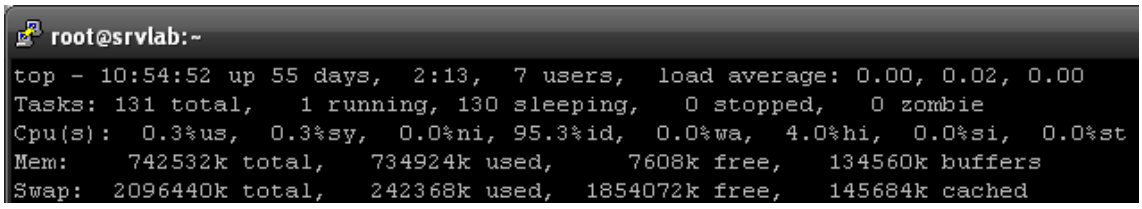
D. PRUEBA DE CONSUMO DE RECURSOS DE ASTERISK

Para corroborar la información disponible en Internet sobre el dimensionamiento de servidores ASTERISK, se ha planteado el siguiente escenario donde se utiliza un servidor ASTERISK para realizar hasta 2 llamadas simultáneas y recibir una, y verificar el impacto en la utilización de recursos del computador. El computador tiene las siguientes características:

- Procesador: Pentium IV de 1.8 Ghz.
- Memoria RAM: 756 Mb.
- Disco duro: 20 Gb.
- Tarjeta de red: 10/100/1000 Mbps.
- Tarjeta de telefonía analógica: OpenVox A400P con 4 puertos FXO.

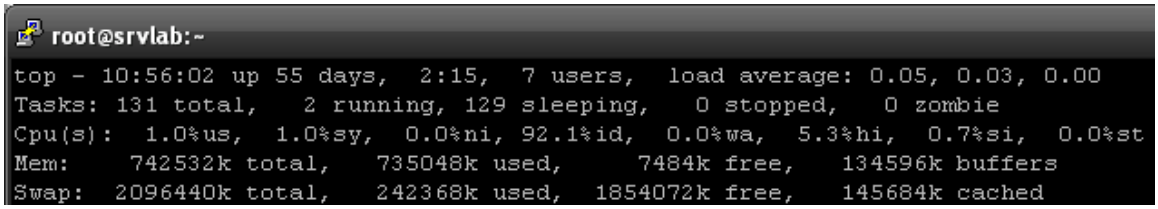
La PBX se encuentra configurada para utilizar códec G711 *ulaw*. Se utilizan hasta 3 líneas de la tarjeta de telefonía analógica simultáneamente. Para visualizar el estado del servidor se utiliza el comando “top” a través de una terminal SSH.

1. Estado del servidor sin procesar llamadas.



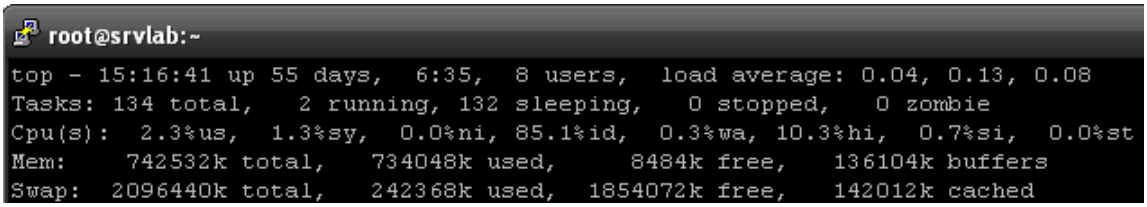
D.1. Vista de los recursos del sistema en el caso 1

2. Estado del servidor al procesar una llamada saliente que es recibida en el servidor. La llamada se origina en un puerto FXO y termina en otro FXO del servidor ASTERISK.



D.2. Vista de los recursos del sistema en el caso 2

3. Estado del servidor al procesar una llamada como la del caso 2, y otro llamada hacia un teléfono en la red pública. Todas las llamadas se realizan de forma simultánea.



D.3. Vista de los recursos del sistema en el caso 3

Se puede visualizar en todos los casos un aumento en el consumo recursos del procesador durante el tiempo que duran las llamadas. Este aumento está alrededor del 7% en promedio, lo cual en este caso equivale a un aproximado de 128 MHz. Esta información concuerda con datos de requisitos para una central telefónica ASTERISK disponibles en Internet.

ANEXO E

PROFORMAS

PROFORMA

Número: 11-0001403 ***Fecha:*** 2011-03-10

Cliente: Super Intendencia de Telecomunicaciones

Atención: Ing.José Béjar

Sistema: Telefonía IP ***Responsable:*** Billy Albán

SideVox pone a su consideración la oferta de los siguientes equipos y/o servicios:

cant.	ítem	v. unitario	v. total
1	Tarjeta de 4 puertos Openvox (A400P)	299.00	299.00
		subtotal:	**299.00**
		iva:	**35.88**
		total:	**334.88**

Condiciones

Forma de pago: 70% de anticipo y el 30% una vez finalizada la instalación.
Validez de la oferta: 7 días.
Garantía: Tres años contra defectos de fabricación en todo el hardware.
Plazo de entrega: 30 días.

Quito, 11 de Marzo del 2011

Atención: José Bejar
SUPERTEL

COTIZACIÓN

TARJETA OPENVOX PCI A400P4

DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
OPENVOX 4 puertos	**1**	**$353.00**	**$353.00**

Overview

OpenVox A400P delivers great voice quality in the telephony systems. With interchangeable FXS/FXO modules, it can eliminate the requirement for separate channel banks or access gateways.

The A400P contains 4 module banks. Each bank supports one analog interface. The module banks may be filled with up to 4 FXO or FXS modules enabling the creation of any combination of ports. Scaling of an analog card solution is accomplished by simply adding additional cards.

A400P works with Asterisk®, Elastix®, FreeSWITCH™, PBX in a Flash, trixbox®, Yate™ and IPPBX/IVR projects as well as other Open Source and proprietary PBX, Switch, IVR, and VoIP gateway applications.

Technical Specifications

- • Up to 4 ports through a combination of FXS and FXO modules

- • 4 RJ-11 interfaces on a single PCI bracket
- • 32 bit 33MHz PCI and fully PCI 2.2 compliant
- • 32 bit bus master DMA data exchanges across PCI interface at 132 Mbytes/sec
- • Autosense compatibility with 5 V and 3.3 V PCI busses compatible
- • Firmware accelerate I/O access to achieve high stability
- • Power: 2.77W Minimum, 11.6W Maximum at 3.3 V or 5 V.
- • Operation temperature: 0°C to 50°C
- • Storage temperature: -40°C to 125°C
- • Dimension: 13.8cm*10.2cm*1.8cm
- • Weight: 82g

- Los precios no incluyen IVA, no incluyen transporte
- La entrega de los equipos es inmediata previo stock caso contrario es de 5 días en tarjeteria
- Estos precios son únicamente para nuestros canales de distribución
- La forma de pago es de contado o con cheque a la fecha, cheque certificado, o transacción bancaria cta. Cte. 05016727.
- **La Garantía de los equipos Grandstream es de 1 año contra defectos de fábrica.**
- A partir de la segunda compra se pueden aplicar créditos adjuntando los requisitos siguientes:

REQUISITOS PARA SER CANAL

- RUC
- DATOS DEL REPRESENTANTE LEGAL
- COPIA DE LA CEDULA DEL REPRESENTANTE LEGAL
- DATOS DE LA EMPRESA(DIRECCION, TELEFONO, FAX,CONTACTO)
- REFERENCIA COMERCIAL Y CERTIFICADO BANCARIO

Espero ayudarle con sus preguntas e inquietudes y gustoso de atenderle.

Michelle Barriga M.
ASESOR COMERCIAL SIBAGAL CIA. LTDA.
Teléfono: (02)323-8591
www.sibagal.com.ec
abarriga@sibagal.com.ec
msn: mishuco87@hotmail.com

Quito, 11 de Marzo del 2011

Atención: Ing. José Bejar
SUPERTEL

COTIZACIÓN

TARJETA OPENVOX PCI express **A400P**4

DESCRIPCION	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
OPENVOX 4 puertos	**1**	**$375.00**	**$375.00**

Especificaciones Tecnicas.

- • Up to 4 ports through a combination of FXS and FXO modules
- • 4 RJ-11 interfaces on a single PCI bracket
- • 32 bit 33MHz PCI and fully PCI 2.2 compliant
- • 32 bit bus master DMA data exchanges across PCI interface at 132 Mbytes/sec
- • Autosense compatibility with 5 V and 3.3 V PCI busses compatible
- • Firmware accelerate I/O access to achieve high stability
- • Power: 2.77W Minimum, 11.6W Maximum at 3.3 V or 5 V.
- • Operation temperature: 0℃ to 50℃
- • Storage temperature: -40℃ to 125℃
- • Dimension: 13.8cm*10.2cm*1.8cm
- • Weight: 82g

Saludos

Javier Mejia
Clear Center/Clearbox
Product Manager

RUC: 1791966740001

COTIZACION No. PN01-0565

Fecha: Quito, 29 de Junio del 2011
Empresa: **SUPERTEL**
Atención: Ing. Jose Bejar
Teléfono:
EMAIL

CANTIDAD	DESCRIPCION	PRECIO	TOTAL
1	TARJETA OPENVOX A400P+4 FXO MODULES [TARXXXA400P40]	426,00	426,00

Validez de la oferta 15 días - Precios sujetos a variación

Subtotal	$ 426,00
12% IVA	$ 51,12
FLETE	
Total	$ 477,12

ENTREGA: 24 horas
GARANTIA: 1 AÑO
PAGO: **CREDITO EMPRESARIAL**
FAVOR GIRAR CHEQUES Y RETENCION A NOMBRE DE:
GRUMANHER S.A.

Atentamente,

Paola Niaupari
VENTAS EMPRESARIAL
Dirección: Av. Eloy Alfaro N32-476 y Pablo Suárez, Esq.
PBX: (02)3238-031 **Extensión:** 1007
Fax: (02)3238042
Cellphone: (09)5270-287
E-mail: pnaupari@saz.com.ec
MSN: pnaupari@saz.com.ec
Web: www.saz.com.ec

ANEXO F

DOCUMENTOS

Quito, 16 de septiembre de 2010

SUPERINTENDENCIA DE TELECOMUNICACIONES
OFICINA MATRIZ
RECEPCION DE DOCUMENTOS
QUITO 21 SEP 2010 9:36 HORA
TRAMITE No. 08357 No. FOJAS: S/A
RECIBIDO POR:

Ing. Fabián Jaramillo
SUPERINTENDENTE DETELECOMUNICACIONES
Presente,

Por su intermedio me dirijo a la SUPERINTENDENCIA DE TELECOMUNICACIONES, organismo de control que tan acertadamente dirige, con el fin de solicitarle de la manera más atenta me facilite información respecto a los delitos que se han cometido en telecomunicaciones en los últimos cinco años en el Ecuador. Esta información la necesito para incluirla en un estudio que me encuentro elaborando para mi proyecto de titulación en la Escuela Politécnica Nacional. Soy estudiante de la carrera de Ingeniería Electrónica y Redes de Información, y mi proyecto de titulación tiene como eje principal el fraude conocido como sistema telefónico "By Pass", por lo cual incluiré un análisis de la situación en los últimos años de este delito en el Ecuador.

La información que solicito puntualmente es la siguiente:

1. Cantidad de sistemas telefónicos "By pass" intervenidos por año, desde el 2005.
2. Modalidades de operación de los sistemas telefónicos "By pass" intervenidos.
3. Perjuicio económico causado por cada sistema telefónico "By pass" intervenido.
4. Operadora de telefonía afectada en cada sistema telefónico "By pass" intervenido.

Esta información de ser posible, en el periodo desde el 2005 hasta su última actualización en el presente año.

Por la atención que preste a la presente y seguro de contar con su valiosa colaboración, anticipo mis agradecimientos.

Atentamente,

Sr. José Béjar Albán.

Oficio IET-2011-00022

Quito, 15 de febrero de 2011

Señor
José Béjar
SOLICITANTE
Urb. Armenia 1, Calle José Javanen; lote 402; Valle de los Chillos
095275747
Quito

Ref. HT.08357

ASUNTO: PEDIDO DE INFORMACIÓN RELACIONADA CON SERVICIOS DE TELEFONÍA INTERNACIONAL NO AUTORIZADO

De mi consideración:

Me refiero a su comunicación ingresada a esta Superintendencia con hoja trámite número 08357 ingresada a esta Institución el 21 de septiembre de 2010, en la que manifiesta que en su calidad de estudiante de la Facultad de Ingeniería en Electrónica y Redes de Información de la Escuela Politécnica Nacional, se encuentra efectuando su Proyecto de Titulación cuyo eje principal está relacionado con los denominados sistemas de telefonía internacional denominados "By pass", razón por la cual solicita información técnica al respecto conforme a los puntos siguientes:

- Sobre la *"Cantidad de sistemas telefónicos "By pass" intervenidos por año, desde el 2005"*, a continuación encontrará la cantidad de intervenciones efectuadas en el periodo solicitado, conforme consta en el "Cuadro 1" siguiente:

INTERVENCIONES A SISTEMAS DE TELEFONÍA INTERNACIONAL TIPO "BY PASS"	
AÑO	CANTIDAD DE INTERVENCIONES REALIZADAS
2005	13
2006	18
2007	15
2008	17
2009	26
2010	40
TOTAL	129

"Cuadro 1"

- Al respecto de las *"Modalidades de operación de los sistemas telefónicos "By pass"* intervenidos", en los párrafos siguientes se describe en forma concreta las diferentes modalidades utilizadas para implementar esa clase de sistemas no autorizados.

Cabe mencionar que, en la implementación y operación de un sistema telefónico tipo "By pass", es necesario contar con la interconexión de los tres elementos tecnológicos siguientes: un enlace digital a través del cual se establece la comunicación internacional; los equipos de telecomunicaciones cuya aplicación específica es el procesamiento de las llamadas internacionales; y, las líneas telefónicas cuyo uso permite terminar de manera no autorizada, en redes nacionales, las llamadas originadas en el exterior.

Los elementos tecnológicos antes descritos, conforme al avance tecnológico han ido evolucionando, hecho que ha repercutido en la modalidad con que esa clase de sistemas se estructura actualmente, de ahí se pueden mencionar las principales modalidades siguientes:

Conforme al uso de líneas telefónicas los sistemas telefónicos "By pass" se han implementado con:

- Líneas telefónicas fijas.
- Líneas telefónicas RDSI.
- Líneas telefónicas móviles.
- Líneas sobre redes HFC.

De acuerdo a los equipos que conforman la instalación de equipos de telecomunicaciones, los sistemas telefónicos "By pass" se han implementado con:

- Equipos para voz sobre "Frame Relay".
- Concentradores telefónicos VoIP.
- "Gateways" de voz para redes fijas.
- "Gateways" de voz para redes móviles.

- "Gateways" de voz GSM.
- "SIM BOX" para almacenamiento de "sim cards".

En cuanto a enlaces digitales, los sistemas telefónicos "By pass", se han implementado con:

- Enlaces satelitales.
- Enlaces dedicados mediante líneas de cobre.
- Enlaces por fibra óptica.
- Enlaces "spread spectrum", punto - multipunto con el uso de antenas omnidireccionales.
- Enlaces sobre redes HFC.
- Enlaces digitales inalámbricos instalados clandestinamente, como extensión de un enlace autorizado.
- Enlaces digitales con tecnología Wi Max.

Resulta necesario mencionar que la operatividad tecnológica de un sistema telefónico "By pass", se encuentra determinada, fundamentalmente, por la forma como se lo estructure, hecho que radica en las múltiples combinaciones que se pueden obtener tomando en cuenta las diversas variantes a las que se puede recurrir frente a los tres elementos que conforman esta clase de sistemas.

- En relación al *"Perjuicio económico causado por cada sistema telefónico "By pass" intervenido"* , se debe manifestar que esta Superintendencia en su calidad de Organismo Técnico de Control, efectúa un cálculo *estimativo* sobre los recursos económicos que se evitaron perder debido a las acciones efectuadas dentro del combate a esta clase de sistemas no autorizados, con esta consideración se presenta el *"Cuadro 2"* a continuación:

INTERVENCIONES A SISTEMAS DE TELEFONÍA INTERNACIONAL TIPO "BY PASS"		
AÑO	CANTIDAD DE INTERVENCIONES REALIZADAS	MONTO ESTIMADO QUE SE EVITÓ PERDER POR ACCIONES DE SUPERTEL (USD$)
2005	13	3.486.033
2006	18	17.609.200
2007	15	8.801.691
2008	17	11.508.109
2009	26	11.646.597
2010	40	15.599.168

"Cuadro 2"

- Con el propósito de atender el punto cuatro de su requerimiento, que textualmente

dice: "Operadora de telefonía afectada en cada sistema telefónico "By pass" intervenido", se ha elaborado el *"Cuadro 3"* que consta a continuación:

INTERVENCIONES A SISTEMAS TELEFÓNICOS "BY PASS" CONFORME A CADA OPERADORA AFECTADA, 2005 - 2010						
OPERADORA	2005	2006	2007	2008	2009	2010
ANDINATEL	2	1	3	2	3	6
PACIFICTEL	7	3	8			
OTECEL	4	5	2	4	6	7
CONECEL		9	1	10	6	20
TELECSA				1	3	6
ECUADORTELECOM					6	
SETEL			1		2	
GLOBAL CROSSING						1
TOTAL	13	18	15	17	26	40

"Cuadro 3"

Finalmente, es necesario manifestar a usted que toda la información que consta en este documento se proporciona en el marco del Proyecto de Titulación que usted se encuentra elaborando en su calidad de estudiante de la Escuela Politécnica Nacional, por esa razón corresponde expresar que el alcance sobre el uso de la misma, se limita única y exclusivamente a la consecución de dicho Proyecto.

Atentamente,

Ing. Julio César Hidalgo
DIRECTOR NACIONAL DE INVESTIGACIÓN ESPECIAL EN TELECOMUNICACIONES

Quito, 18 enero de 2011

Ing. Julio César Hidalgo
DIRECTOR NACIONAL DE INVESTIGACIÓN ESPECIAL EN TELECOMUNICACIONES
Presente,

Me dirijo a usted con el fin de solicitarle de la manera más atenta me facilite información respecto al tráfico telefónico de larga distancia internacional (LDI) en los últimos 3 años en el Ecuador. Esta información la necesito para incluirla en un estudio que me encuentro elaborando para mi proyecto de titulación en la Escuela Politécnica Nacional. Soy estudiante de la carrera de Ingeniería Electrónica y Redes de Información, y mi proyecto de titulación tiene como eje principal el fraude conocido como sistema telefónico "By Pass", por lo cual incluiré un análisis de la situación en los últimos años de este delito en el Ecuador.

La información que solicito puntualmente es la siguiente:

1. Volumen de tráfico entrante y saliente de larga distancia internacional cursados por mes, durante los años 2008, 2009 y 2010 consolidado por telefonía móvil y fija.
2. Cantidad total de llamadas entrantes y salientes de larga distancia internacional cursadas por mes, durante los años 2008, 2009 y 2010 consolidado por telefonía móvil y fija.

Por la atención que preste a la presente y seguro de contar con su valiosa colaboración, anticipo mis agradecimientos.

SUPERTEL
SUPERINTENDENCIA DE TELECOMUNICACIONES
OFICINA MATRIZ
RECEPCION DE DOCUMENTOS
QUITO 18 ENE 2011 HORA 14:48
TRAMITE No.: 00804 No. FOJAS: 5 1/2
RECIBIDO POR:

Atentamente,

Sr. José Béjar Albán
C.I. 1717527871
Teléfono: (02)2341617
Celular: 095275747
Dirección: Urb. La Armenia 1, Calle José Javanen, Lote 402.
e-Mail: josebejar87@hotmail.com

Oficio DIE-2011-00059

Quito, 29 de abril del 2011

Señor
José Béjar
Estudiante de Ingeniería en Electrónica y Redes de Información
ESCUELA POLITÉCNICA NACIONAL
Quito

ASUNTO : ATENDER PEDIDO DE INFORMACIÓN RELACIONADO CON SERVICIOS DE TELEFONÍA.

De mi consideración:

Me refiero a su comunicación ingresada a esta Superintendencia con hoja de control y trámite número 00802, en la que manifiesta que en su calidad de estudiante de la Facultad de Ingeniería en Electrónica y Redes de Información de la Escuela Politécnica Nacional, se encuentra efectuando su Proyecto de Titulación cuyo eje principal está relacionado con los denominados sistemas de telefonía internacional denominados "By pass", razón por la cual solicita información técnica al respecto conforme a los puntos siguientes:

1.- Volumen de tráfico entrante y saliente de larga distancia internacional cursados por mes, durante los años 2008, 2009 y 2010, consolidado por telefonía móvil y fija.

2.- Cantidad total de llamadas entrantes y salientes de larga distancia internacional cursadas por mes, durante los años 2008, 2009, y 2010, consolidado por telefonía móvil y fija.

La información requerida se entrega adjunta a este documento, en los cuadros que contienen la información solicitada conforme a los dos puntos descritos.

Finalmente, es necesario manifestar a usted que toda la información que se adjunta a este documento se proporciona en el marco del Proyecto de Titulación que usted se encuentra elaborando en su calidad de estudiante de la Escuela Politécnica Nacional, por esa razón corresponde expresar que el alcance sobre el uso de la misma, se limita única y exclusivamente a la consecución de dicho Proyecto.

Atentamente,

Ing. Julio César Hidalgo
DIRECTOR NACIONAL DE INVESTIGACIÓN ESPECIAL EN TELECOMUNICACIONES

			Ene-08	Feb-08	Mar-08	Abr-08	May-08	Jun-08	Jul-08	Ago-08	Sep-08	Oct-08	Nov-08	Dic-08
OPERADORES - FIJOS	TTIE	llamadas	8.052.232	7.593.377	8.246.924	7.951.044	8.527.652	8.058.843	8.112.773	7.817.081	8.590.082	7.638.837	7.114.639	7.949.922
OPERADORES - FIJOS	TTIS	llamadas	1.778.848	1.672.309	1.783.540	1.845.955	1.909.961	1.821.071	1.959.556	1.894.177	1.893.299	1.882.745	1.782.103	1.966.515
OPERADORES - MÓVILES	TTIE	llamadas	9.176.578	8.699.876	9.414.855	8.916.073	9.353.211	8.777.611	9.008.880	8.983.948	9.076.370	8.935.229	8.720.264	9.382.794
OPERADORES - MÓVILES	TTIS	llamadas	8.153.018	7.575.160	8.384.766	8.045.966	8.747.405	8.681.107	9.144.565	9.231.616	9.038.578	9.145.392	8.949.534	10.408.988

			Ene-09	Feb-09	Mar-09	Abr-09	May-09	Jun-09	Jul-09	Ago-09	Sep-09	Oct-09	Nov-09	Dic-09
OPERADORES - FIJOS	TTIE	llamadas	7.608.892	6.505.339	7.143.372	6.789.761	7.208.128	6.827.401	6.940.931	6.847.198	6.648.614	6.376.912	6.042.046	6.915.796
OPERADORES - FIJOS	TTIS	llamadas	2.147.957	1.967.925	2.143.679	2.182.677	2.116.638	2.070.180	2.073.442	1.974.117	1.866.281	1.853.181	1.706.176	1.899.022
OPERADORES - MÓVILES	TTIE	llamadas	9.292.739	8.285.783	9.292.862	8.660.022	9.223.165	8.734.041	9.067.490	9.341.121	8.824.480	9.036.220	8.697.927	9.736.097
OPERADORES - MÓVILES	TTIS	llamadas	9.114.115	8.170.138	9.358.787	8.364.776	9.043.051	8.954.814	9.066.421	9.176.969	8.896.870	9.234.764	9.148.850	10.962.135

			Ene-10	Feb-10	Mar-10	Abr-10	May-10	Jun-10	Jul-10	Ago-10	Sep-10	Oct-10	Nov-10	Dic-10
OPERADORES - FIJOS	TTIE	llamadas	6.562.262	5.861.967	6.186.757	5.918.315	6.809.632	6.240.964	6.193.019	6.847.760	6.449.070	6.430.888	6.155.770	6.876.781
OPERADORES - FIJOS	TTIS	llamadas	1.774.285	1.650.918	1.893.037	1.712.103	1.828.784	1.741.067	1.818.788	1.849.003	1.839.111	1.814.499	1.739.177	1.896.092
OPERADORES - MÓVILES	TTIE	llamadas	9.154.521	8.322.706	9.048.612	8.575.851	8.924.878	8.256.838	8.819.622	9.367.464	8.951.780	8.941.469	8.424.814	9.496.302
OPERADORES - MÓVILES	TTIS	llamadas	9.561.652	8.495.643	9.370.658	8.224.881	8.928.080	8.505.731	8.876.139	9.330.978	8.188.113	8.450.028	9.264.548	10.284.798

			Ene-08	Feb-08	Mar-08	Abr-08	May-08	Jun-08	Jul-08	Ago-08	Sep-08	Oct-08	Nov-08	Dic-08
OPERADORES - FIJOS	TTIE	minutos	88.430.357	80.094.066	87.988.980	83.903.177	85.628.214	81.796.124	85.259.226	84.942.976	83.595.875	82.654.010	78.573.830	85.213.857
OPERADORES - FIJOS	TTIS	minutos	7.628.996	7.349.527	8.085.553	8.289.443	8.378.474	8.218.995	8.751.316	8.654.446	8.758.710	8.689.876	8.398.788	8.816.544
OPERADORES - MÓVILES	TTIE	minutos	57.447.173	51.535.585	54.659.860	54.373.984	54.586.012	54.075.660	54.927.484	56.446.549	54.966.038	54.624.168	52.752.844	55.491.870
OPERADORES - MÓVILES	TTIS	minutos	17.189.554	15.344.370	16.600.219	16.041.711	17.837.052	17.232.503	18.043.960	18.076.947	18.136.354	19.148.469	17.626.008	20.709.758

			Ene-09	Feb-09	Mar-09	Abr-09	May-09	Jun-09	Jul-09	Ago-09	Sep-09	Oct-09	Nov-09	Dic-09
OPERADORES - FIJOS	TTIE	minutos	79.525.470	68.527.368	78.143.610	73.455.741	79.247.778	73.604.189	74.789.552	76.029.647	72.341.637	71.166.729	67.818.196	74.100.620
OPERADORES - FIJOS	TTIS	minutos	9.921.244	8.768.702	9.766.844	9.191.414	9.423.343	9.295.926	9.091.707	8.837.903	8.641.280	8.615.100	8.119.396	8.353.202
OPERADORES - MÓVILES	TTIE	minutos	55.132.735	48.214.016	53.516.128	49.741.920	52.499.316	51.053.459	52.809.346	53.281.207	50.907.914	50.668.846	50.254.928	53.968.638
OPERADORES - MÓVILES	TTIS	minutos	17.810.737	15.810.680	19.030.464	15.868.429	17.973.539	17.560.502	17.396.771	17.063.070	16.128.542	17.041.765	17.775.557	22.044.517

			Ene-10	Feb-10	Mar-10	Abr-10	May-10	Jun-10	Jul-10	Ago-10	Sep-10	Oct-10	Nov-10	Dic-10
OPERADORES - FIJOS	TTIE	minutos	72.691.498	62.769.594	67.675.165	62.876.075	67.413.389	63.554.231	64.295.069	70.866.544	67.733.818	68.336.164	65.730.538	71.549.422
OPERADORES - FIJOS	TTIS	minutos	8.224.581	7.577.221	8.812.273	8.029.204	8.348.596	7.970.452	8.101.982	8.260.020	8.378.033	8.396.575	7.804.784	8.281.235
OPERADORES - MÓVILES	TTIE	minutos	53.107.061	48.207.369	53.434.509	49.521.195	50.577.162	47.415.635	49.602.496	51.379.117	48.762.254	49.604.217	47.832.249	52.128.379
OPERADORES - MÓVILES	TTIS	minutos	17.834.341	15.904.329	17.367.559	15.675.250	17.877.700	15.909.873	16.207.900	16.420.649	15.434.016	15.503.378	15.673.027	18.562.456