



REPÚBLICA DEL ECUADOR

Escuela Politécnica Nacional

" E S C I E N T I A H O M I N I S S A L U S "

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

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

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

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

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

Respeto hacia sí mismo y hacia los demás.

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REINGENIERÍA DE LA RED DE DATOS CORPORATIVA DE LA EMPRESA ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A. PARA LA INTEGRACIÓN DE SERVICIOS DE TELEFONÍA IP

TOMO I

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

MORALES MARTÍNEZ FRANCISCO JAVIER
nido_rano@lycos.com

SARABIA JÁCOME DAVID FERNANDO
dfsarabia@gmail.com

DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO.
phidalgo@ieee.org

QUITO, NOVIEMBRE 2011

DECLARACIÓN

Nosotros, Francisco Javier Morales Martínez, David Fernando Sarabia Jácome, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros 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.

Francisco Javier Morales Martínez

David Fernando Sarabia Jácome

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Francisco Javier Morales Martínez y David Fernando Sarabia Jácome, bajo mi supervisión.

Ing. Pablo Hidalgo L.
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a Dios, por darme la salud, la inteligencia y la fuerza para alcanzar ésta y otras tantas metas que me depara el futuro.

A mis padres y hermanos, por estar conmigo siempre apoyándome.

A David “*Vivín*”, mi compañero de proyecto, por su actitud positiva y su paciencia.

A mis profesores, en especial a mi director, Ing. Pablo Hidalgo, que siempre nos alentó a buscar la excelencia.

A mis amigos y familiares, por sus valiosos consejos e ideas.

A todos ellos, mi infinita gratitud.

Francisco J. Morales Martínez

AGRADECIMIENTO

A Dios, por brindarme esta segunda oportunidad de vivir, por la sabiduría, fuerza y paciencia concedida durante mi carrera universitaria.

A mis padres y hermanos, por su apoyo y esfuerzo diario, por estar siempre conmigo en los momentos difíciles vividos durante el desarrollo de este proyecto.

A mi director, el Ing. Pablo Hidalgo por sus consejos desinteresados y su paciencia para guiar responsablemente y de la mejor manera el presente proyecto.

A mi compañero de tesis, Francisco “Doc”, por su apoyo brindado en los momentos difíciles, por tenerme paciencia y por el esfuerzo brindado para sacar este proyecto adelante.

A Alianza de Seguros, por haber confiado en nosotros y sobre todo por abrirnos las puertas y brindarnos una oportunidad para demostrar los conocimientos adquiridos en las aulas. Al Ing. Pablo Herrera por creer en nosotros y por su apoyo incondicional.

A mis familiares y amigos que siempre creyeron en mí y me brindaban fuerzas para continuar luchando y no desmayar.

Esto es de ellos, esto es por ellos y para ellos, gracias por su apoyo.

David F. Sarabia Jácome

DEDICATORIA

Esta labor va dedicada a todas y cada una de esas personas que el destino puso en mi camino, en especial a aquellas que me acompañan hoy por hoy, me llenan de ánimo y me enseñan lo que es verdaderamente importante en la vida.

A mi mami Tina,

A mi papi Santos,

A mis ñaños, Patty y Sou,

A ti, mi *amorcito corazón*...

A mis mejores amigas, Monilú, Karilú y Melú,

A mis amigos de siempre,

A todos los que no recuerda mi memoria pero sí mi corazón.

Francisco J. Morales Martínez

DEDICATORIA

A mis padres, Edgar Daniel Gustavo y Laura Josefina, que cada día me inspiran y me apoyan en todo para alcanzar mis metas. Les amo.

A mis hermanos, Aleja, Maite y Pepe Lucho, que recuerden que los sueños son alcanzables con perseverancia y constancia. Éste es un camino a seguir y a superar. Les quiero mucho.

A mis familiares y amigos, que siempre estuvieron alentándome para lograr mis objetivos.

David F. Sarabia Jácome

CONTENIDO

DECLARACIÓN.....	ii
CERTIFICACIÓN.....	iii
AGRADECIMIENTO.....	iv
DEDICATORIA.....	vi
CONTENIDO.....	viii
RESUMEN.....	xxii
PRESENTACIÓN.....	xxiv

ÍNDICE GENERAL

TOMO I

CAPÍTULO 1

1. FUNDAMENTOS DE REDES DE DATOS Y TELEFONÍA IP	1
1.1 REDES DE DATOS	1
1.1.1 CLASIFICACIÓN.....	1
1.1.1.1 Por el Medio de Transmisión.....	1
1.1.1.2 Por su Cobertura	2
1.1.2 TOPOLOGÍAS	2
1.1.3 MODELO ISO/OSI.....	3
1.1.3.1 Capa Física.....	3
1.1.3.2 Capa Enlace	4
1.1.3.3 Capa Red.....	4
1.1.3.4 Capa Transporte	4
1.1.3.5 Capa Sesión	4
1.1.3.6 Capa Presentación	4
1.1.3.7 Capa Aplicación.....	5
1.1.4 REDES LAN	5
1.1.4.1 Tecnologías de Medio Compartido.....	5
1.1.4.2 Control de Acceso al Medio	6
1.1.4.3 Tecnologías Conmutadas.....	6
1.1.4.4 Redes LAN de Alta Velocidad	7
1.1.4.5 Trama IEEE 802.3	8
1.1.4.6 VLAN	9
1.1.5 CABLEADO ESTRUCTURADO	10
1.1.5.1 Estándares de Cableado Estructurado.....	11
1.1.5.2 Categorías de Cable para Cableado Estructurado.....	12
1.1.6 REDES WAN.....	12
1.1.6.1 Tecnologías WAN.....	13

1.1.6.1.1	Frame-Relay	13
1.1.6.1.2	ATM (Asynchronous Transfer Mode)	14
1.1.6.1.3	MPLS (MultiProtocol Label Switching)	14
1.1.7	EQUIPOS DE CONECTIVIDAD	14
1.1.7.1	Hub	15
1.1.7.2	Bridge	15
1.1.7.3	Switch	15
1.1.7.4	Router	16
1.1.7.5	Gateway	16
1.1.8	ARQUITECTURA TCP/IP	16
1.1.8.1	Protocolo IP	18
1.1.8.1.1	Direccionamiento IP	19
1.1.8.2	Protocolos TCP Y UDP	19
1.1.9	MODELO CLIENTE – SERVIDOR Y APLICACIONES DE RED	20
1.2	TELEFONÍA TRADICIONAL	21
1.2.1	SISTEMAS TELEFÓNICOS TRADICIONALES	21
1.2.1.1	PSTN (Public Switched Telephone Network)	22
1.2.1.2	PBX (Private Branch eXchange)	23
1.2.2	CONMUTACIÓN DE CIRCUITOS	23
1.2.3	TELEFONÍA ANALÓGICA Y DIGITAL	24
1.2.4	ETAPAS DE UNA LLAMADA TELEFÓNICA	25
1.2.5	SEÑALIZACIÓN	25
1.2.6	SERVICIOS	26
1.2.7	LIMITACIONES DE LA TELEFONÍA TRADICIONAL	27
1.3	TELEFONÍA IP	28
1.3.1	DIGITALIZACIÓN DE LA VOZ Y CÓDECS DE AUDIO	28
1.3.1.1	VoIP, Voz sobre IP	30
1.3.1.2	Características de Telefonía IP	31
1.3.2	RECOMENDACIÓN H.323	32
1.3.2.1	Arquitectura H.323	32
1.3.2.2	Protocolos H.323	33
1.3.2.3	Establecimiento de una Llamada H.323	34
1.3.2.4	Terminación de una Llamada H.323	36
1.3.3	SIP (Session Initiation Protocol)	37
1.3.3.1	Funciones de SIP	38
1.3.3.2	Arquitectura SIP	38
1.3.3.3	SDP (Session Description Protocol)	40
1.3.3.4	Establecimiento de Sesiones SIP	40
1.3.3.4.1	Registro SIP	41
1.3.3.4.2	Rol del Servidor Proxy	42
1.3.3.4.3	Rol del Servidor de Redirección	43
1.3.4	COMPARACIÓN ENTRE SIP Y H.323	44
1.3.5	PROTOS DE TRANSPORTE A TIEMPO REAL: RTP Y RTCP	45
1.3.5.1	RTP (Real-Time Transport Protocol)	45
1.3.5.2	RTCP (RTP Control Protocol)	46
1.3.6	CALIDAD DE SERVICIO (QoS) EN REDES BASADAS EN IP	47
1.3.6.1	IntServ (Integrated Services)	48
1.3.6.1.1	RSVP (Resource reSerVation Protocol)	49
1.3.6.2	DiffServ (Differentiated Services)	51
1.3.6.3	Encolamiento Priorizado	52
1.3.6.3.1	Colas de Prioridad	53
1.3.6.3.2	WFQ (Weighted Fair Queuing)	54
1.3.6.3.3	CBQ (Class-Based Queuing)	54
1.3.6.4	Ingeniería de Tráfico con MPLS	55

1.3.7	COMUNICACIONES UNIFICADAS.....	56
1.3.7.1	Mensajería Unificada.....	57
1.3.7.2	Colaboración en Tiempo Real	57
1.3.7.3	Presencia.....	58
1.3.7.4	Servicios en Comunicaciones Unificadas.....	58
1.3.7.5	Aplicaciones con Comunicaciones Unificadas.....	60
REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 1.....		63

CAPÍTULO 2

2.	ANÁLISIS DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS.....	68
2.1	ANÁLISIS DE LA SITUACIÓN ACTUAL.....	68
2.1.1	ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A.	68
2.1.1.1	Misión	68
2.1.1.2	Visión.....	68
2.1.1.3	Situación Actual de Alianza de Seguros.....	69
2.1.1.3.1	<i>Distribución de las Instalaciones en Quito y Guayaquil</i>	69
2.1.1.3.2	<i>Estructura organizacional de Alianza de Seguros</i>	71
2.1.1.3.3	<i>Características del Personal de Alianza</i>	72
2.1.2	ANÁLISIS DE LA RED DE DATOS.....	75
2.1.2.1	Antecedentes.....	75
2.1.2.2	Red LAN.....	76
2.1.2.2.1	<i>Sistema de Cableado Estructurado</i>	76
2.1.2.2.2	<i>Equipos de Conectividad</i>	80
2.1.2.2.3	<i>Servidores</i>	81
2.1.2.2.4	<i>Dispositivos Terminales</i>	84
2.1.2.2.5	<i>Direccionamiento IP</i>	85
2.1.2.3	Red WAN	86
2.1.2.3.1	<i>Equipos WAN</i>	87
2.1.2.3.2	<i>Enlaces WAN</i>	88
2.1.2.3.3	<i>Acuerdos de Nivel de Servicio</i>	88
2.1.2.4	Servicios y Aplicaciones de Red	89
2.1.2.4.1	<i>Bases de Datos</i>	90
2.1.2.4.2	<i>Antivirus</i>	91
2.1.2.4.3	<i>Servicio de Aplicaciones</i>	91
2.1.2.4.4	<i>Escritorio Remoto</i>	93
2.1.2.4.5	<i>Correo electrónico</i>	94
2.1.2.4.6	<i>Compartición de Archivos</i>	94
2.1.2.4.7	<i>WEB</i>	95
2.1.2.4.8	<i>DNS</i>	95
2.1.2.4.9	<i>DHCP</i>	96
2.1.2.4.10	<i>Firewall</i>	96
2.1.2.4.11	<i>Directorio Activo</i>	97
2.1.2.4.12	<i>Video – Vigilancia</i>	97
2.1.2.5	Enrutamiento.....	98
2.1.2.6	Análisis de Tráfico.....	100
2.1.2.6.1	<i>Enlace WAN Quito</i>	100
2.1.2.6.2	<i>Enlace WAN Guayaquil-Centro</i>	103
2.1.2.6.3	<i>Enlaces hacia los servidores</i>	104
2.1.2.6.4	<i>Protocolos</i>	106
2.1.3	ANÁLISIS DE LA RED TELEFÓNICA.....	107

2.1.3.1	Infraestructura Telefónica en Quito y Guayaquil	108
2.1.3.1.1	Central Telefónica de Quito.....	108
2.1.3.1.2	Central Telefónica de Guayaquil-centro	111
2.1.3.1.3	Cableado Telefónico	113
2.1.3.1.4	Terminales Telefónicos	114
2.1.3.1.5	Interconexión con la PSTN.....	116
2.1.3.2	Análisis de Tráfico de Voz	117
2.2	RESULTADOS DEL ANÁLISIS DE LA SITUACIÓN ACTUAL	120
2.2.1	RENDIMIENTO	121
2.2.2	ESCALABILIDAD	122
2.2.3	DISPONIBILIDAD.....	123
2.2.4	ADMINISTRACIÓN	124
2.2.5	CALIDAD DE SERVICIO	125
2.2.6	SEGURIDAD	125
2.3	ANÁLISIS DE REQUERIMIENTOS	126
2.3.1	REQUERIMIENTOS PARA LAS REDES LAN DE QUITO Y GUAYAQUIL	126
2.3.1.1	Infraestructura de cableado estructurado	126
2.3.1.2	Estructura de la red LAN	127
2.3.2	REQUERIMIENTOS PARA la INTEGRACIÓN DE VOZ Y DATOS.....	128
2.3.2.1	Funciones del Sistema de Telefonía IP.....	129
2.3.2.2	Análisis y Elección de Códecs.....	130
2.3.3	REQUERIMIENTOS PARA EL ENLACE WAN Y CONEXIÓN CON LA PSTN.....	133
2.3.3.1	Llamadas Simultáneas entre Sucursales	133
2.3.3.2	Tipo y número de circuitos troncales hacia la PSTN.....	134
2.3.4	CRECIMIENTO DE USUARIOS	135
2.3.4.1	Proyección de usuarios de datos	136
2.3.4.2	Proyección de usuarios de voz.....	137
2.3.5	PROYECCIONES DEL TRÁFICO DE RED.....	138
2.3.5.1	Ancho de banda requerido por servicio	138
2.3.5.1.1	Base de Datos	139
2.3.5.1.2	Servicio de Aplicaciones.....	140
2.3.5.1.3	Escritorio Remoto	140
2.3.5.1.4	Acceso a Internet	141
2.3.5.1.5	Correo Electrónico	142
2.3.5.1.6	Compartición de Archivos	143
2.3.5.1.7	Video Vigilancia	144
2.3.5.1.8	Antivirus.....	146
2.3.5.1.9	Llamada IP	148
2.3.5.2	Ancho de Banda requerido según la simultaneidad de usuarios y servicios	149
2.3.5.3	Ancho de banda estimado para <i>backbone</i> de las redes LAN Quito y Guayaquil.....	152
REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 2		153

CAPÍTULO 3

3. DISEÑO DE LA RED DE DATOS Y TELEFONÍA IP, SOLUCIONES DE TELEFONÍA IP	158
3.1 ESQUEMA DE REINGENIERÍA PROPUESTO	158

3.1.1	MODELO JERÁRQUICO	159
3.2	DISEÑO DE LAS REDES LAN QUITO Y GUAYAQUIL CON SERVICIOS INTEGRADOS DE TELEFONÍA IP	161
3.2.1	SISTEMA DE CABLEADO ESTRUCTURADO PARA QUITO	161
3.2.1.1	Áreas de Trabajo.....	162
3.2.1.2	Cuarto de Equipos.....	162
3.2.1.3	Cuarto de Telecomunicaciones.....	164
3.2.1.4	Cableado Horizontal	165
3.2.1.4.1	<i>Categoría a Utilizar</i>	165
3.2.1.4.2	<i>Rutas de Cableado</i>	166
3.2.1.5	Cableado Vertical	167
3.2.1.5.1	<i>Categoría a Utilizar</i>	167
3.2.1.5.2	<i>Rutas de Backbone</i>	167
3.2.1.6	Dimensionamiento de los elementos para el Cableado Estructurado	168
3.2.1.6.1	<i>Dimensionamiento de elementos para Rutas de Cableado</i>	169
3.2.1.6.2	<i>Cálculo del número de rollos de cable</i>	170
3.2.2	DISEÑO DE LA RED ACTIVA DE QUITO Y GUAYAQUIL	172
3.2.2.1	Elementos Activos de la Red.....	172
3.2.2.1.1	<i>Dispositivos Terminales</i>	173
3.2.2.1.2	<i>Equipos de Conectividad</i>	173
3.2.2.1.3	<i>Servidores</i>	174
3.2.2.2	Conectividad.....	174
3.2.2.2.1	<i>Capa de Acceso</i>	174
3.2.2.2.2	<i>Capa de Distribución</i>	175
3.2.2.2.3	<i>Capa de Núcleo</i>	177
3.2.2.3	Diseño Lógico de la Red.....	178
3.2.2.3.1	<i>Direccionamiento IP</i>	179
3.2.2.3.2	<i>VLANs</i>	180
3.2.2.3.3	<i>Enrutamiento entre VLANs</i>	180
3.2.2.3.4	<i>Plan de Numeración</i>	181
3.2.2.3.5	<i>Categorización de Usuarios</i>	182
3.2.2.3.6	<i>Grupos de usuarios telefónicos</i>	183
3.2.3	SERVICIOS Y APLICACIONES.....	184
3.2.3.1	Reorganización de los Servicios y Aplicaciones Existentes.....	185
3.2.3.1.1	<i>Base de Datos</i>	185
3.2.3.1.2	<i>Antivirus</i>	186
3.2.3.1.3	<i>Correo Electrónico</i>	186
3.2.3.1.4	<i>Compartición de archivos</i>	187
3.2.3.1.5	<i>DHCP, DNS, y Directorio</i>	188
3.2.3.2	Servicio de Telefonía IP, Colaboración y Comunicaciones Unificadas... ..	188
3.2.3.2.1	<i>Descripción del servicio de Telefonía IP</i>	189
3.2.3.2.2	<i>Prestaciones básicas de Telefonía relacionadas con las llamadas</i>	191
3.2.3.2.3	<i>Mensajería Unificada</i>	191
3.2.3.2.4	<i>Integración con otros servicios de red</i>	193
3.2.3.2.5	<i>Servicios opcionales y futuros de comunicaciones unificadas</i>	194
3.2.4	DIMENSIONAMIENTO DE EQUIPOS DE LA RED LAN	195
3.2.4.1	Servidores	195
3.2.4.1.1	<i>Servidor de aplicaciones Thin-Client</i>	196
3.2.4.1.2	<i>Servidor de Antivirus McAfee</i>	197
3.2.4.1.3	<i>Servidor de Correo</i>	197
3.2.4.1.4	<i>Servidor de Archivos</i>	197
3.2.4.1.5	<i>Servidor IPT</i>	198
3.2.4.2	<i>Gateways de Voz</i>	199

3.2.4.3	Switches	199
3.2.4.3.1	Dimensionamiento de switches de capa acceso.....	200
3.2.4.3.2	Dimensionamiento de switches de capa distribución	200
3.2.4.3.3	Dimensionamiento de switches capa de núcleo.....	201
3.2.4.3.4	Dimensionamiento de la velocidad de backplane y throughput	202
3.2.4.4	Terminales Telefónicos IP	203
3.2.5	DIAGRAMA DE RED.....	204
3.3	DIMENSIONAMIENTO DEL ENLACE WAN QUITO-GUAYAQUIL Y ACCESO A LA PSTN	204
3.3.1	UBICACIÓN DE LAS SUCURSALES	206
3.3.2	DIMENSIONAMIENTO DE ENLACES	206
3.3.2.1	Tolerancia a Errores.....	207
3.3.2.2	Sensibilidad al Retardo	207
3.3.2.3	Ancho de Banda.....	207
3.3.3	TECNOLOGÍA WAN A UTILIZARSE.....	210
3.3.4	CAPACIDAD DEL ENLACE WAN.....	212
3.3.5	CONDICIONES DE SERVICIO PARA EL SLA	213
3.3.6	ACCESO A LA PSTN	214
3.4	DISPONIBILIDAD	214
3.4.1	REDUNDANCIA EN LA RED CORPORATIVA.....	215
3.4.2	SUMINISTRO DE ENERGÍA ELÉCTRICA Y AIRE ACONDICIONADO	217
3.4.2.1	PoE (<i>Power over Ethernet</i>).....	217
3.4.2.2	UPS (<i>Uninterruptible Power Supply</i>).....	218
3.4.2.3	Planta de Energía Eléctrica a Diesel	218
3.4.2.4	Aire Acondicionado	219
3.5	CALIDAD DE SERVICIO	219
3.5.1	SEGMENTACIÓN Y PRIORIZACIÓN DE TRÁFICO	220
3.5.2	RETARDOS	222
3.5.2.1	Codificación de la Voz	222
3.5.2.2	Encolamiento	222
3.5.2.3	Serialización	223
3.5.2.4	<i>Buffer de Jitter</i>	223
3.5.3	APROVISIONAMIENTO DE RECURSOS	223
3.6	ADMINISTRACIÓN DE LA RED.....	224
3.6.1	SNMP	225
3.6.2	HERRAMIENTAS DE GESTIÓN	225
3.6.3	POLÍTICAS DE ADMINISTRACIÓN DE RED	226
3.6.4	Administración del Cableado Estructurado.....	227
3.7	SEGURIDAD	227
3.7.1	<i>FIREWALL</i> Y SISTEMA DE DETECCIÓN DE INSTRUSOS, IDS.....	228
3.7.2	<i>SIP TRUNKING</i> SEGURO.....	229
3.7.3	POLÍTICAS DE SEGURIDAD DE RED	229
3.7.3.1	Análisis de Riesgos de Red.....	230
3.7.3.2	Normas del buen uso de recursos de red.....	231
3.7.3.2.1	<i>Normativas de acceso</i>	231
3.7.3.2.2	<i>Normativas de seguridad de acceso físico</i>	232
3.7.3.2.3	<i>Normativas de servicios de red</i>	232
3.7.3.2.4	<i>Normativas para el manejo de información</i>	233
3.7.3.2.5	<i>Normativas de software y hardware</i>	234
3.8	SOLUCIONES DE TELEFONÍA IP	234
3.8.1	SELECCIÓN DEL ESTÁNDAR PARA TELEFONÍA IP	235
3.8.2	DIRECTRICES DE PRESELECCIÓN PARA LA SOLUCIÓN DE TELEFONÍA IP	235

3.8.3	CISCO	236
3.8.3.1	<i>Media Convergence Server</i> MCS-7828-I5	237
3.8.3.2	<i>Cisco Unified Communications Manager</i> 8.5 (UCM).....	237
3.8.3.3	<i>Cisco Unity Connection</i> 8.5 (UC).....	238
3.8.3.4	Terminales Telefónicos	238
3.8.3.5	Solución <i>Cisco</i> para <i>Routers</i> como <i>Media Gateways</i>	239
3.8.4	<i>HP Networking</i>	239
3.8.4.1	Servidor <i>HP VCX v7005</i>	240
3.8.4.2	<i>Software</i> de Comunicaciones Unificadas <i>VCX 9.5</i>	240
3.8.4.3	Terminales Telefónicos y <i>Gateways</i> de Voz	241
3.8.4.4	Solución <i>HP</i> para <i>Routers</i> como <i>Media Gateways</i>	241
3.8.5	AVAYA	242
3.8.5.1	<i>IP Office Control Unit</i> 500v2.....	242
3.8.5.2	<i>IP Office Manager</i> 9.0	243
3.8.5.3	<i>VoiceMail Pro</i>	243
3.8.5.4	Terminales Telefónicos	244
3.8.6	ANÁLISIS Y SELECCIÓN DE LA SOLUCIÓN DE TELEFONÍA IP	244
3.9	RESUMEN DE REQUERIMIENTOS DE MATERIALES Y EQUIPOS.....	246
3.9.1	EQUIPOS DE CONECTIVIDAD REUTILIZABLES	246
REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 3.....		248

TOMO II

CAPÍTULO 4

4. ANÁLISIS DE COSTOS	254	
4.1	COSTO DE LA RED PASIVA	254
4.2	COSTO DE LA RED ACTIVA	254
4.2.1	SOLUCIÓN DE TELEFONÍA IP	255
4.2.1.1	<i>Hardware</i> y <i>software</i>	255
4.2.1.2	Licencias	259
4.2.1.3	Condiciones de Soporte y Mantenimiento Anual	261
4.2.1.4	Garantía, Instalación y Costo Total de la Solución de Telefonía IP	262
4.2.2	SOLUCIÓN DE CONECTIVIDAD	262
4.2.2.1	Equipos de Conectividad	263
4.2.2.2	Soporte y Mantenimiento Anual.....	265
4.2.2.3	Instalación, Garantía y Costo Total de la Solución de Conectividad.....	265
4.3	SERVICIO DE TRANSPORTE DE DATOS	266
4.3.1	COSTOS DE ENLACES	266
4.3.2	ACUERDOS DE SERVICIO Y OPERACIÓN	267
4.4	TRONCALES SIP	267
4.5	SERVIDORES	268
4.6	PERSPECTIVAS DE RETORNO DE LA INVERSIÓN	269
4.6.1	INGRESOS	269
4.6.2	COSTOS DE INVERSIÓN.....	271
4.6.3	COSTOS DE OPERACIÓN Y MANTENIMIENTO	272
4.6.4	FLUJO DE FONDOS.....	272
4.6.5	RENTABILIDAD	273
REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 4.....		276

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES	278
5.1 CONCLUSIONES	278
5.2 RECOMENDACIONES	282

ÍNDICE DE FIGURAS

CAPÍTULO 1

Figura 1.1	Capas del modelo ISO/OSI	3
Figura 1.2	Trama IEEE 802.3	8
Figura 1.3	Trama IEEE 802.3 con campo para VLANs	9
Figura 1.4	Relación entre las capas del modelo ISO/OSI y de la arquitectura TCP/IP	17
Figura 1.5	Estructura del paquete IPv4	19
Figura 1.6	Funcionamiento del modelo Cliente - Servidor	20
Figura 1.7	Representación del sistema telefónico de la PSTN	22
Figura 1.8	Componentes de la Arquitectura H.323	32
Figura 1.9	Funcionamiento de un <i>gateway</i> de voz	33
Figura 1.10	Establecimiento de una llamada H.323 con señalización enrutada por el <i>gatekeeper</i>	36
Figura 1.11	Establecimiento de una llamada directa sin <i>gatekeeper</i>	37
Figura 1.12	Establecimiento de una sesión SIP simple entre dos terminales	40
Figura 1.13	Registro de un Agente de Usuario con el Servidor Registrar	42
Figura 1.14	Establecimiento de una sesión SIP mediante el servidor <i>Proxy</i>	42
Figura 1.15	Establecimiento de una sesión SIP mediante el servidor de Redirección	43
Figura 1.16	<i>Stack</i> de protocolos H.323	44
Figura 1.17	<i>Stack</i> de protocolos SIP	44
Figura 1.18	Funcionamiento de RTP	47
Figura 1.19	Proceso de Reserva RSVP	50
Figura 1.20	Diferenciación de tráfico en el borde de la red con DiffServ	51
Figura 1.21	Combinación entre DiffServ e IntServ	52
Figura 1.22	Diagrama de flujo de colas de priorización	53
Figura 1.23	Diagrama de flujo de colas WFQ	54
Figura 1.24	Diagrama de flujo de colas CBQ	55
Figura 1.25	Ventajas de una infraestructura de comunicaciones IP	61
Figura 1.26	Telepresencia	62

CAPÍTULO 2

Figura 2.1	Instalaciones de Alianza en Quito	69
Figura 2.2	Castillo Larrea. Oficinas de Alianza en Quito.....	70
Figura 2.3	Estructura organizacional de Alianza de Seguros	72
Figura 2.4	Distribución de cableado estructurado Quito	77
Figura 2.5	Distribución de equipos en los <i>racks</i> de Quito	78
Figura 2.6	Distribución de equipos en los <i>racks</i> de Guayaquil.....	79
Figura 2.7	Esquema topológico de las LAN UIO y GYE.....	82
Figura 2.8	Funcionamiento del servicio de antivirus <i>McAfee</i> en Alianza.....	92
Figura 2.9	Configuración actual de las direcciones IP en la Red Corporativa de Alianza.....	99
Figura 2.10	Tráfico de entrada y salida del enlace WAN Quito, periodo febrero-mayo 2010	101
Figura 2.11	Semana de mayor tráfico del enlace WAN Quito del 8 al 14 de marzo 2010.....	102
Figura 2.12	Semana de mayor tráfico del enlace WAN Guayaquil del 22 al 29 de marzo 2010	103
Figura 2.13	Porcentaje de utilización de los protocolos	107
Figura 2.14	PBX's Panasonic KX-TD1232 de Alianza de Seguros con sus respectivos módulos de extensiones y líneas troncales	110
Figura 2.15	PBX's Panasonic KX-TD1232 de Alianza de Seguros con sus respectivas tarjetas internas de interconexión y DISA	110
Figura 2.16	PBX Alcatel <i>Office PRO4200</i> con sus respectivos.....	112
Figura 2.17	Rangos de frecuencia de banda estrecha y banda ancha.....	131
Figura 2.18	Número de usuarios simultáneos del servidor de base de datos. Semana del 22 al 29 de marzo 2010.....	140

CAPÍTULO 3

Figura 3.1	Esquema general para el diseño de red propuesto	159
Figura 3.2	Estándares T568A y T56B para conectores RJ-45	163
Figura 3.3	<i>Patch panel</i>	164
Figura 3.4	Distribución de los cuartos de equipos y de telecomunicaciones.....	165
Figura 3.5	Elementos de cableado estructurado en el área de trabajo.....	166
Figura 3.6	Rutas de Cableado Vertical	168
Figura 3.7	Conexión entre las capas distribución y acceso.....	176
Figura 3.8	Conexiones entre las capas núcleo y distribución	177
Figura 3.9	Diagrama lógico del funcionamiento de VLANs	181
Figura 3.10	Elementos de Telefonía IP dentro de la red corporativa.....	190
Figura 3.11	Gateway HP VCX v7111 FXO/FXS y Cisco ATA 187.....	199
Figura 3.12	Topología propuesta para la Red Corporativa de Alianza de Seguros	205
Figura 3.13	Esquema de enlaces WAN	211
Figura 3.14	Priorización de tráfico a través de la red corporativa	222
Figura 3.15	Servidor de Telefonía IP Cisco MCS-7828-I5	238

Figura 3.16	Teléfonos IP Cisco serie 7900.....	239
Figura 3.17	Teléfonos IP HP serie 3500 y 3100. Servidor HP VCX v7005.....	241
Figura 3.18	Avaya IP <i>Office control unit</i> 500v2. Vista posterior.....	243

CAPÍTULO 4

Figura 4.1	Servidor Cisco MCS 7828.....	257
Figura 4.2	Teléfono IP Cisco 7942G. Pantalla de los teléfonos IP.....	257
Figura 4.3	Vista posterior de Cisco ATA187 y dispositivos compatibles.....	258
Figura 4.4	<i>Router</i> Cisco 2901. Vistas frontal y posterior.....	259
Figura 4.5	<i>Switches</i> de acceso Cisco WS-C2960-24PC-S y WS-C2960-48PST-S.....	263
Figura 4.6	<i>Switch</i> de distribución Cisco WS-C2960G-24TC-L.....	263
Figura 4.7	<i>Switch</i> de núcleo Cisco WS-C3560G-24TS-S.....	264
Figura 4.8	<i>Servidor HP Proliant</i> DL360G7. Vistas Frontal y Posterior.....	268

ÍNDICE DE TABLAS

CAPÍTULO 1

Tabla 1.1	Características de las categorías de cable UTP.....	12
Tabla 1.2	Características de códecs para la transmisión de voz.....	29

CAPÍTULO 2

Tabla 2.1	Distribución de ambientes y departamentos en Quito.....	70
Tabla 2.2	Distribución de ambientes y departamentos en Guayaquil – Centro.....	71
Tabla 2.3	Número de empleados de Alianza.....	73
Tabla 2.4	Distribución del personal en Alianza Quito.....	74
Tabla 2.5	Distribución del personal en Alianza Guayaquil.....	74
Tabla 2.6	Distribución de puntos de red en Alianza – Quito.....	77
Tabla 2.7	Número de usuarios y número de equipos terminales.....	79
Tabla 2.8	Equipos de conectividad LAN Quito.....	80
Tabla 2.9	Equipos de conectividad LAN Guayaquil.....	81
Tabla 2.10	Características de los servidores y sus correspondientes servicios.....	83
Tabla 2.11	Total de dispositivos terminales de la red en Quito y Guayaquil.....	85
Tabla 2.12	Características de los dispositivos terminales.....	85
Tabla 2.13	Direccionamiento IP de la Red Corporativa de Alianza.....	86
Tabla 2.14	Equipos de conectividad WAN QUITO.....	87
Tabla 2.15	Equipos de conectividad WAN GUAYAQUIL.....	87
Tabla 2.16	Enlaces de transmisión de datos y acceso a Internet.....	88
Tabla 2.17	Planeación de direccionamiento IP para enrutamiento.....	98

Tabla 2.18	Volumen de tráfico semanal enlace WAN Quito tomado entre Febrero y Mayo de 2010.....	102
Tabla 2.19	Velocidad máxima de entrada y salida del Enlace WAN Quito.....	103
Tabla 2.20	Velocidad máxima de entrada y salida del enlace WAN de Guayaquil	104
Tabla 2.21	Volumen de tráfico de los servidores	104
Tabla 2.22	Velocidad máxima de los enlaces hacia los servidores	105
Tabla 2.23	Tarjetas ocupadas en la central telefónica y sus puertos	113
Tabla 2.24	Terminales telefónicos en Alianza Quito	115
Tabla 2.25	Terminales telefónicos en Alianza Guayaquil.....	116
Tabla 2.26	Resumen de líneas telefónicas de Quito y Guayaquil	116
Tabla 2.27	Tipo de llamadas y su distribución diaria.....	118
Tabla 2.28	Porcentaje de llamadas y su distribución horaria	119
Tabla 2.29	Volumen e Intensidad de tráfico telefónico.....	120
Tabla 2.30	Códecs de audio para Telefonía IP	131
Tabla 2.31	Tráfico proyectado y circuitos recomendados.....	133
Tabla 2.32	Proyección de tráfico en 5 años.....	134
Tabla 2.33	Resumen de líneas troncales a utilizarse	135
Tabla 2.34	Crecimiento estimado del personal de Alianza en 5 años	136
Tabla 2.35	Crecimiento de usuarios de red de datos	136
Tabla 2.36	Número y tipo de usuarios de voz para Quito y Guayaquil.....	137
Tabla 2.37	Crecimiento de usuarios de voz.....	138
Tabla 2.38	Estadísticas de las transacciones realizadas por hora entre un cliente y el servidor de la base de datos	139
Tabla 2.39	Volumen de información del servicio de correo electrónico en el intervalo de una semana	142
Tabla 2.40	Opciones de video disponibles en el servidor de video <i>Digiguard</i> DG0412 para el sistema NTSC	145
Tabla 2.41	Velocidad de transmisión para diferentes combinaciones de video con MPEG-4.....	145
Tabla 2.42	Ancho de banda requerido para Telefonía IP en las redes LAN Quito y Guayaquil y enlace WAN.....	150
Tabla 2.43	Proyección de tráfico en 5 años para cada servicio de datos.....	151
Tabla 2.44	Ancho de banda para backbone en redes LAN Quito y Guayaquil.....	152

CAPÍTULO 3

Tabla 3.1	Resumen de Puntos de datos y voz por piso.....	163
Tabla 3.2	Capacidad de Tubería Conduit para cable UTP de 6.1 mm de diámetro según norma ANSI-EIA/TIA 569 A	169
Tabla 3.3	Capacidad de escalerillas y canaletas estándar para cables UTP de 6.1 mm de diámetro	170
Tabla 3.4	Rollos de cable UTP cat 6 necesarios para el cableado horizontal.....	171
Tabla 3.5	Detalle de cable UTP para cableado vertical.....	172

Tabla 3.6	Direccionamiento IP de subredes	179
Tabla 3.7	Segmentación de VLANs	180
Tabla 3.8	Plan de numeración propuesto para Telefonía IP	181
Tabla 3.9	Perfil de usuarios telefónicos de Alianza de Seguros	182
Tabla 3.10	Ubicación y ámbito de los servicios existentes en la red corporativa	186
Tabla 3.11	Prestaciones básicas del servicio telefónico	192
Tabla 3.12	Cantidad de switches de acceso y números de puertos correspondientes	200
Tabla 3.13	Conexión y números de puertos para el switch de distribución	201
Tabla 3.14	Cantidad de puertos para los <i>switches</i> de núcleo.....	202
Tabla 3.15	Resumen de las velocidades de <i>backplane</i> y <i>throughput</i> requerido	203
Tabla 3.16	Número de terminales telefónicos IP.....	204
Tabla 3.17	Ubicación y crecimiento de las sucursales de Alianza	206
Tabla 3.18	Tipo de tráfico a cursar por la red WAN y sus características	207
Tabla 3.19	Ancho de banda requerido según el servicio de red para el	209
Tabla 3.20	Resumen de las capacidades necesarias para todos los enlaces hacia el <i>carrier</i>	212
Tabla 3.21	Resumen del tráfico generado por la matriz de Quito hacia Internet	212
Tabla 3.22	Clasificación de PSE y PD en el estándar IEEE 802.3af.....	217
Tabla 3.23	Valores de prioridad del protocolo 802.1p	220
Tabla 3.24	Equivalencia entre valores CoS y DSCP	221
Tabla 3.25	Recursos de Red a proteger	230
Tabla 3.26	Resumen de los posibles atacantes de recursos de red	231
Tabla 3.27	Condiciones para los <i>switches</i> de posible reutilización	247

CAPÍTULO 4

Figura 4.1	Servidor Cisco MCS 7828	257
Figura 4.2	Teléfono IP Cisco 7942G. Pantalla de los teléfonos IP	257
Figura 4.3	Vista posterior de Cisco ATA187 y dispositivos compatibles.....	258
Figura 4.4	Router Cisco 2901. Vistas frontal y posterior	259
Figura 4.5	Switches de acceso Cisco WS-C2960-24PC-S y WS-C2960-48PST-S	263
Figura 4.6	Switch de distribución Cisco WS-C2960G-24TC-L.....	263
Figura 4.7	Switch de núcleo Cisco WS-C3560G-24TS-S.....	264
Figura 4.8	Servidor HP Proliant DL360G7. Vistas Frontal y Posterior	268

ANEXOS

ANEXO A DISTRIBUCIÓN DE ÁREAS DE TRABAJO EN ALIANZA QUITO
ANEXO B ACUERDOS DE NIVEL DE SERVICIO CON MEGADATOS S.A

ANEXO C TRÁFICO DE ENLACES DE SUCURSALES Y SERVIDORES

ANEXO C.1 TRÁFICO DE SUCURSALES
ANEXO C.2 TRÁFICO DE SERVIDORES

- ANEXO D MODELO DE ENCUESTA DE SERVICIO TELEFÓNICO
- ANEXO E CÁLCULO DE INTENSIDAD DE TRAFICO TELEFÓNICO PARA LA CIUDAD DE QUITO Y GUAYAQUIL
- ANEXO F PÁGINAS WEB AUTORIZADAS CON SU RESPECTIVO TAMAÑO Y TIEMPO DE DESCARGA

- ANEXO G
 - ANEXO G.1 PLANOS DE CABLEADO ESTRUCTURADO
 - ANEXO G. 2 DIMENSIONAMIENTO DE RACKS
 - ANEXO G. 3 DISTANCIA DE LOS PUNTOS DE RED

- ANEXO H INFORMACIÓN DE LOS PROCESOS ACTUALES Y SU OCUPACIÓN DE MEMORIA RAM DE LOS SERVIDORES DE ANTIVIRUS Y APLICACIONES

- ANEXO I CÁLCULO *BACKPLANE* Y *THROUGHPUT* PARA *SWITCHES*

- ANEXO J CÁLCULO DE LOS ENLACES WAN PARA EL RESTO DE SUCURSALES

- ANEXO K DIMENSIONAMIENTO DE UPS Y AIRE ACONDICIONADO

- ANEXO L REQUERIMIENTOS PARA MATERIALES Y EQUIPOS DE LA RED CORPORATIVA
 - ANEXO L.1 MATERIALES DE CABLEADO ESTRUCTURADO
 - ANEXO L.2 MATRIZ DE COMPARACIÓN ENTRE LAS PLATAFORMAS DE COMUNICACIONES UNIFICADAS: *CISCO UCMBE5Kv8.5*, *HP VCX V7005* Y *AVAYA IP OFFICE R7.0*
 - ANEXO L.3 REQUERIMIENTOS PARA EQUIPOS DE CONECTIVIDAD Y CUMPLIMIENTO DE LA MARCA CISCO
 - ANEXO L.4 REQUERIMIENTOS PARA LOS SERVIDORES DE ANTIVIRUS, *THIN-CLIENT*, CORREO ELECTRÓNICOS Y DE ARCHIVOS
 - ANEXO L.5 REQUERIMIENTOS PARA TELÉFONOS IP Y CUMPLIMIENTO DE LA MARCA CISCO

- ANEXO M CARACTERÍSTICAS *SWITCH 3COM 4200*

- ANEXO N COTIZACIONES Y PRECIOS REFERENCIALES
 - ANEXO N.1 COTIZACIÓN DE CABLEADO ESTRUCTURADO
 - ANEXO N.2 COTIZACIÓN DE LA PLATAFORMA DE TELEFONÍA IP *CUCMBE5Kv8.5*
 - ANEXO N.3 COTIZACIÓN DE EQUIPOS DE CONECTIVIDAD MARCA CISCO
 - ANEXO N.4 COTIZACIÓN DE EQUIPOS DE CONECTIVIDAD MARCA D-LINK
 - ANEXO N.5 COTIZACIÓN DE EQUIPOS DE CONECTIVIDAD MARCA HP

- ANEXO N.6 COTIZACIÓN DE ENLACES WAN
- ANEXO N.7 PRECIOS REFERENCIALES DE TRONCALES SIP
- ANEXO N.8 COTIZACIÓN SERVIDORES *HP PROLIANT*

ANEXO O ESPECIFICACIONES TÉCNICAS

- ANEXO O.1 ESPECIFICACIONES TÉCNICAS *CISCO UNIFIED COMMUNICATIONS MANAGER BUSINESS EDITION 5000 v8.5*
- ANEXO O.2 ESPECIFICACIONES TÉCNICAS SERVIDOR *CISCO MCS7828-15*
- ANEXO O.3 ESPECIFICACIONES TÉCNICAS *CISCO UNIFIED COMMUNICATIONS MANAGER v8.5*
- ANEXO O.4 ESPECIFICACIONES TÉCNICAS *CISCO UNITY CONNECTION v8.5*
- ANEXO O.5 ESPECIFICACIONES TÉCNICAS TELÉFONO IP *CISCO 7942G*
- ANEXO O.6 ESPECIFICACIONES TÉCNICAS TELÉFONO IP *CISCO 7911G*
- ANEXO O.7 ESPECIFICACIONES TÉCNICAS TELÉFONO IP *CISCO 7962G*
- ANEXO O.8 ESPECIFICACIONES TÉCNICAS *ROUTER CISCO 2901*
- ANEXO O.9 ESPECIFICACIONES TÉCNICAS SERVIDOR *HP PROLIANT DL360 G7*

RESUMEN

En el presente proyecto se realiza la reingeniería de la red de datos corporativa para la empresa Alianza de Seguros y Reaseguros S.A., con el objetivo de incluir servicios de telefonía IP.

El primer capítulo contiene los fundamentos teóricos en los cuales se cimenta la reingeniería. Se abordan conceptos relativos a redes LAN, WAN, Telefonía analógica y digital, Telefonía IP y Comunicaciones Unificadas desde una óptica sencilla para entender del desarrollo de este proyecto.

El segundo capítulo presenta el análisis de la situación actual de Alianza de Seguros. Se analizan aspectos como: la estructura organizacional de la compañía, la infraestructura física de las sucursales de Quito y Guayaquil-centro, el sistema de cableado estructurado, los servicios, aplicaciones y equipos de la red, el sistema telefónico privado, etc. Este capítulo también contiene el análisis de tráfico para los enlaces de sucursales y servidores. Se presenta una breve evaluación sobre el estado actual de la red y los requerimientos para mejorar el desempeño de los servicios actuales y para implantar los nuevos servicios de Telefonía IP.

En el tercer capítulo se procede con el desarrollo de la reingeniería de la red. Se plantea el rediseño del sistema de cableado estructurado para Quito. Se establece el nuevo esquema de la red activa, detallando el funcionamiento y el redimensionamiento de equipos de conectividad, servidores y equipos terminales. Se plantea el redimensionamiento y la reorganización de los servicios de red, y el funcionamiento de los nuevos servicios de Telefonía IP. Se realiza el dimensionamiento del enlace WAN. Se presentan las características de disponibilidad, calidad de servicio, seguridad y administración consideradas para la red. Se procede con la selección de la solución de Telefonía IP, en base al análisis de plataformas de las marcas: Cisco, HP y Avaya.

El cuarto capítulo contiene el desglose y el análisis de costos para todos los componentes que se requieren como producto de la reingeniería. Se desglosan los costos de materiales, equipos de red, enlaces y servicios, así como los costos de soporte, mantenimiento e instalación en base a proformas de distintos distribuidores y proveedores nacionales. Se determina la rentabilidad del proyecto mediante el flujo de fondos para 5 años.

Las conclusiones y recomendaciones generadas a lo largo del proyecto se plasman en el quinto capítulo.

En la parte final de este trabajo se presentan los anexos que contienen tablas, figuras, ejemplos de cálculo, cotizaciones, especificaciones técnicas de equipos y otros documentos que complementan y aclaran el contenido de los cinco capítulos anteriores.

PRESENTACIÓN

Distintas empresas y organizaciones a nivel mundial obtienen importantes beneficios con el uso de los avances tecnológicos que presentan, sobre todo, las redes de comunicaciones. Uno de los avances más provechosos para las empresas es la convergencia de voz, datos y video en la misma red, debido a que permite un contacto más directo entre la empresa y el cliente, a la vez que facilita el manejo de la tecnología. De esta forma mejora la satisfacción del cliente y se generan mayores ingresos para las empresas. Éstas son algunas de las metas que persigue Alianza de Seguros.

Alianza de Seguros presenta las condiciones organizacionales y de infraestructura propicias para beneficiarse de los servicios de Telefonía IP. El constante contacto con su clientela y la ubicación de sus sucursales a lo largo del país motivan a la empresa a cambiar los servicios telefónicos tradicionales por los de Telefonía IP aprovechando la infraestructura de la red de datos. Con la Telefonía IP y el rediseño de la red, Alianza de Seguros reducirá los costos por consumo telefónico, simplificará la administración de la red y estará en capacidad de atender a su clientela de una manera más ágil y eficaz.

Con este proyecto se dota a Alianza de Seguros con una infraestructura de comunicaciones lo suficientemente robusta que pueda utilizar todas las ventajas de la Telefonía IP. Adicionalmente, puede evolucionar hacia las Comunicaciones Unificadas o brindar cualquier otro servicio de red con una mínima actualización tecnológica, protegiendo la inversión de la empresa.

Este trabajo puede utilizarse como guía durante la fase de planeamiento para un proyecto de Telefonía IP y Comunicaciones Unificadas, por lo que cualquier empresa, institución o individuos puede verse beneficiado de su contenido, adaptándolo a su situación particular. Se destacan temas como disponibilidad, calidad de servicio, seguridad y administración, por lo que este trabajo ayudaría a estructurar o reestructurar cualquier red convergente, enfocándose a las de tipo empresarial.

CAPÍTULO 1

FUNDAMENTOS DE REDES DE DATOS Y TELEFONÍA IP

1.1 REDES DE DATOS ^{[1][2]}

En los últimos años, las redes de datos han crecido de manera acelerada y se encuentran en una etapa de convergencia de servicios. De esta manera se posibilita que datos, voz y video interactúen en una misma red.

Una red de datos es la interconexión de varios dispositivos que comparten recursos a través del uso de algún medio de transmisión. El objetivo principal de las redes es la disponibilidad de los recursos para cualquier usuario que se encuentre conectado a ellas, sin importar su ubicación física o la de los recursos.

De forma general los elementos que intervienen en una red son: medio de transmisión, equipos de conectividad y terminales o *hosts*. Los equipos de conectividad unen a los terminales a través de medios de transmisión. Los dispositivos terminales permiten a los usuarios interactuar entre sí dentro de la red.

1.1.1 CLASIFICACIÓN ^[2]

Las redes de datos se las puede dividir de acuerdo al medio de transmisión y según su cobertura.

1.1.1.1 Por el Medio de Transmisión ^[2]

Existen dos tipos de redes según el medio de transmisión: cableadas e inalámbricas. En el primer grupo se encuentran todas las tecnologías que utilizan algún medio físico guiado, como el cobre o la fibra óptica, que sirve de camino para las señales. En el segundo grupo se encuentran las tecnologías que emiten

sus señales libremente por el espacio; su principal inconveniente es que estas señales son altamente vulnerables a interferencias.

1.1.1.2 Por su Cobertura ^[2]

La cobertura de las redes de datos viene dada por el área a la que pueden servir. Es así que existen redes que cubren unos pocos metros de distancia y otras que tienen alcance mundial. El rango de cobertura que una red puede abarcar es variable; esto dificulta la clasificación exacta de las redes por este criterio. Existen dos grandes grupos de redes que se pueden identificar: las Redes de Área Local (LAN) y las Redes de Área Extendida (WAN).

Dentro de las LAN se pueden considerar redes que se encuentran en pequeñas localidades o en edificios empresariales. Las WAN pueden estar formadas por la interconexión de diferentes LAN que se encuentran en distintas ubicaciones geográficas expandiendo así su alcance.

1.1.2 TOPOLOGÍAS ^[2]

Las topologías de red han evolucionado en forma y complejidad desde su inicio hasta el día de hoy. Particularmente se han destacado las siguientes topologías: bus, anillo, estrella y árbol. De las anteriores existen variaciones o mezclas, pero la topología en estrella es la más utilizada en redes de datos.

La topología en estrella consiste de un nodo central de comunicaciones al cual se conectan los distintos dispositivos para integrarse en la red, y compartir recursos. El nodo central o *hub*, es el dispositivo por el que fluye toda la información intercambiada entre los dispositivos. La topología en estrella es la más simple de implementar y monitorear; sin embargo, si el nodo central falla se pierde toda conectividad.

1.1.3 MODELO ISO/OSI ^[1]

El modelo de referencia de Sistemas Abiertos Interconectados (OSI, por sus siglas en inglés) fue desarrollado por la Organización Internacional para la Estandarización (ISO, por sus siglas en francés) como una abstracción de las funciones que puede cumplir una red. Dichas funciones están repartidas en 7 capas para facilitar el estudio, entendimiento y operación de las redes.

Las capas que conforman el modelo ISO/OSI se muestran en la figura 1.1 y se describen a continuación:

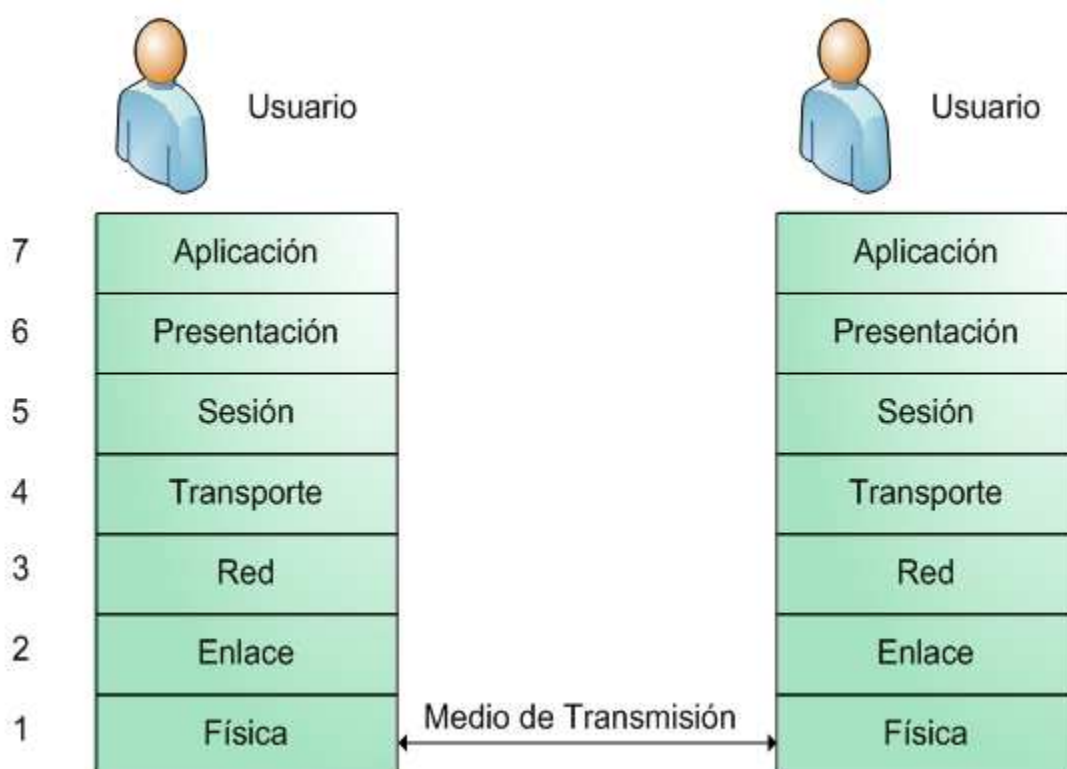


Figura 1.1 Capas del modelo ISO/OSI

1.1.3.1 Capa Física ^[2]

Su principal función es la transmisión de los bits, unos y ceros lógicos, haciendo uso de un medio de transmisión. Define las características funcionales, mecánicas y eléctricas de las interfaces a utilizar.

1.1.3.2 Capa Enlace ^[2]

Establece un enlace lógico entre dos nodos adyacentes. Las principales funciones de esta capa son: la organización de los bits en tramas, el control de errores de transmisión y el control de flujo.

1.1.3.3 Capa Red ^[2]

Su unidad de información es el paquete. La capa red se encarga del enrutamiento de los paquetes, a través de redes heterogéneas desde el origen hasta el destino. Resuelve los problemas de capa enlace.

1.1.3.4 Capa Transporte ^{[1][2][3]}

Esta capa realiza la interconexión *host-host*. Establece o libera conexiones a través de la subred y aísla a las capas superiores de los cambios inevitables de *hardware*. De ser necesario divide los datos recibidos en partes más pequeñas y se asegura que lleguen correctamente al *host* destino.

1.1.3.5 Capa Sesión ^{[1][2][3][4]}

La capa sesión se encarga de manejar múltiples peticiones de conexiones entrantes y salientes de un *host* mediante sesiones. Establece puntos de referencia para continuar transmisiones en caso de interrupción.

1.1.3.6 Capa Presentación ^{[1][2][3][4]}

Posibilita el entendimiento entre *hosts* que pueden tener diferentes formas de representar los datos. Se encarga de dar un formato a las estructuras de datos con una representación estándar para que viajen por la red y sean interpretados en el otro extremo.

1.1.3.7 Capa Aplicación ^{[1][2][3][4]}

Es la interfaz entre el *host* y el usuario. Facilita al usuario el entendimiento de la información que cruza por la red.

Los mensajes de información se generan en la capa aplicación y se entregan a cada una de las capas inferiores consecutivamente hasta llegar al medio físico. Es responsabilidad de cada capa añadir información de control para proveer un servicio y aislar de los detalles de su funcionamiento a la capa superior. Este proceso se conoce como encapsulación.

1.1.4 REDES LAN

Las redes han evolucionado conjuntamente con sus tecnologías, pero la tecnología que más acogida tiene hasta el día de hoy en redes empresariales es *Ethernet* en sus distintas variantes. Las tecnologías *Ethernet* pasaron de ser de medio compartido a ser conmutadas.

1.1.4.1 Tecnologías de Medio Compartido ^[2]

Ethernet nace del uso de un medio alámbrico compartido entre diferentes *hosts*, tecnología que fue estandarizada con algunas variantes por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE por sus siglas en inglés) bajo el grupo de trabajo IEEE 802.3. A diferencia de *Ethernet*, IEEE 802.3 ha tenido un desarrollo continuo hasta la actualidad con significativos avances.

En el estándar IEEE 802.3 se definen las características físicas y de funcionamiento de los elementos que intervienen en estas redes. El primer medio compartido en estas redes fue el cable coaxial grueso que permitía velocidades de hasta 10 Mbps con segmentos de 500 m. Esta red es conocida como 10Base5 y tiene una topología tipo bus. Esta red cambió a cable coaxial delgado con la misma velocidad pero con segmentos de 185 m, denominándose como 10Base2 o IEEE 802.3a.

A partir del estándar IEEE 802.3i o 10Base-T se cambia el medio de transmisión a par trenzado, manteniendo la velocidad de 10 Mbps. La topología cambió a estrella mediante el uso de *hubs*. La distancia máxima permitida es de 100 m comprendidos desde el *hub* al *host* o estación de trabajo.

1.1.4.2 Control de Acceso al Medio ^{[1][2]}

Las tecnologías antes mencionadas hacen uso del mismo medio para la transmisión de información de cada uno de los *hosts*. Esto implica que si dos o más estaciones transmiten simultáneamente por el mismo medio se producirá una colisión, lo cual define un dominio de colisión. De esta manera disminuye el rendimiento de la red y la capacidad de los enlaces es subutilizada.

Para aumentar el rendimiento en redes que utilizan medio compartido se emplea el mecanismo de Acceso Múltiple por Escucha de Portadora y Detección de Colisiones (CSMA/CD por sus siglas en inglés).

En CSMA/CD, mientras se está transmitiendo una trama por el medio, las demás estaciones la escuchan y se abstienen de enviar mensajes. Si el medio está libre y dos o más estaciones envían un mensaje al mismo tiempo se produce una colisión. Las estaciones involucradas emiten una señal conocida como *jamming* para alertar a las demás estaciones que comparten el medio que se produjo una colisión. Tras la colisión las estaciones involucradas esperan un tiempo aleatorio para volver a transmitir.

1.1.4.3 Tecnologías Conmutadas ^{[1][2]}

A medida que se aumentan estaciones, las redes de medio compartido se saturan a pesar del uso de CSMA/CD o el aumento en la velocidad. La solución para aumentar el rendimiento en las redes LAN fue omitir la compartición del medio y así eliminar las colisiones.

En una red conmutada se mantiene la topología en estrella, pero se reemplaza al *hub* como nodo central por un *switch*. Cada puerto del *switch* forma un dominio de colisión independiente de los otros. A diferencia de un *hub*, cuando el *switch* recibe una trama por un puerto, no lo retransmite a los puertos restantes, sino que basado en la dirección destino de la trama la reenvía a la estación adecuada. El *switch* lee las direcciones de origen y destino de las tramas que ingresan a sus puertos, las filtra y forma una tabla de conmutación. Esta tabla contiene la asociación entre la estación y el puerto del *switch* al que se encuentra conectada.

El enlace establecido entre una estación y un puerto del *switch* puede ser un canal *half-duplex* ó *full-duplex*. En un canal *full-duplex* es posible la transmisión y recepción simultáneas.

1.1.4.4 Redes LAN de Alta Velocidad ^{[1][2][3][4]}

Con la introducción de la conmutación en las redes LAN se logró el máximo rendimiento del medio de transmisión. No obstante, las velocidades seguían manteniéndose bajas para los requerimientos, en el orden de los 10 Mbps.

Con el aumento de la capacidad de procesamiento y almacenamiento de las estaciones, se generan nuevas aplicaciones que requieren mayores velocidades de transmisión.

Así nacen nuevos estándares de red con el objetivo de aumentar la velocidad de transmisión, pero condicionados a ser compatibles con los estándares previos. IEEE 803.u establece una velocidad nominal de 100 Mbps con algunas modificaciones en la capa física para el uso de fibra y cobre. De este estándar la versión más conocida es la 100 Base-TX que establece el uso de par trenzado y se lo asocia comúnmente con el término *Fast Ethernet*.

Un salto posterior es la introducción de *Gigabit Ethernet* con una velocidad de 1000 Mbps. *Gigabit Ethernet* se estandariza en IEEE 802.3z e IEEE 802.3ab, sobre fibra y cobre respectivamente. A partir de este estándar se prefiere el

empleo de *switches* en vez de *hubs* para hacer uso de todo el potencial de la red en modo *full-duplex*.

En la actualidad existen otros estándares cuyo objetivo principal es el aumento de la velocidad, tales como IEEE 802.3ae e IEEE 802.3an para fibra óptica y par trenzado respectivamente.

1.1.4.5 Trama IEEE 802.3 ^[2]

IEEE 802.3 trabaja en las dos primeras capas del modelo ISO/OSI: Física y Enlace de datos. Como se ha indicado previamente, en la capa Enlace se organizan los bits en estructuras conocidas como tramas, como se muestra en la figura 1.2.

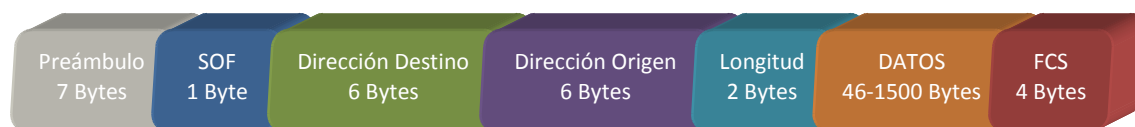


Figura 1.2 Trama IEEE 802.3

Los campos que conforman la trama IEEE 802.3 son:

- **PREÁMBULO.** Consta de 7 bytes con un patrón de 1s y 0s intercalados.
- **SOF (*Start Of Frame*).** Es el byte delimitador que sirve para sincronización. La secuencia binaria es 10101011.
- **DIRECCIÓN DE DESTINO Y DIRECCIÓN ORIGEN.** Cada uno de estos campos consta de 6 bytes que constituyen las direcciones MAC (*Medium Access Control*). La dirección de origen es única e identifica a la estación que emite el mensaje. La dirección destino identifica a la estación o las estaciones receptoras del mensaje emitido.
- **LONGITUD.** Campo de 2 bytes indica la cantidad de bytes del campo datos.
- **DATOS.** Campo de 46 a 1500 bytes que contiene la información recibida de la capa superior.

- **FCS (Frame Check Sequence).** Campo de 4 bytes que realiza la detección de errores en la trama mediante el algoritmo CRC.

1.1.4.6 VLAN ^{[32][33][34][35]}

En un dominio de *broadcast* los mensajes enviados por un dispositivo llegan a todos los dispositivos que conforman un segmento. Al incrementar el número de máquinas en un segmento estos mensajes provocan saturación. Las VLANS (LAN virtuales) son interconexiones virtuales entre distintos dispositivos que dividen dominios físicos en varios dominios lógicos, mejorando el rendimiento de la red.

El protocolo estandarizado para VLAN es el IEEE802.1Q. Define la adición de un campo de 4 bytes en la trama IEEE802.3, donde se ubicarán los *tags* o identificadores de VLANS correspondientes y otros campos de control, como muestra la figura 1.3. Los números de identificación de una VLAN se dividen en los rangos: normal, de 1-1005 y ampliado, de 1006-4094. El rango comprendido entre 1002 y 1005 es reservado para las tecnologías Token Ring y FDDI (*Fiber Distribution Data Interface*).

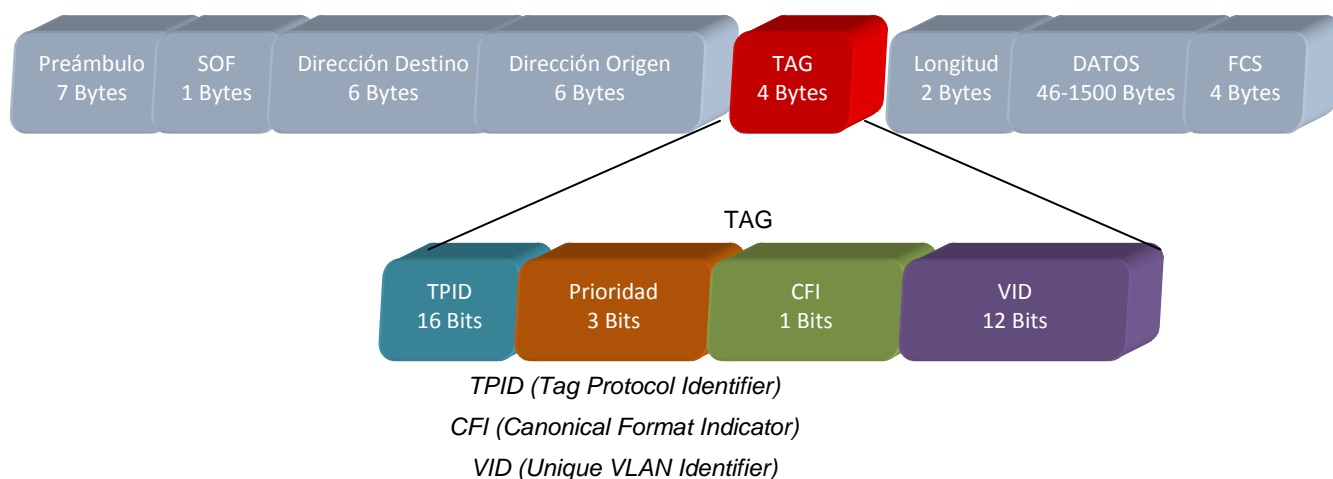


Figura 1.3 Trama IEEE 802.3 con campo para VLANs

Campos del *tag* de una VLAN:

- **TPID.** Campo de 16 bits utilizado para identificar el tipo de protocolo.
- **Prioridad.** Campo de 3 bits utilizado por el estándar 802.1p.
- **CFI.** Campo de 1 bit brinda la facilidad de que tramas Token Ring se envíen a través de los enlaces *Ethernet*.
- **VID.** Campo de 12 bits. Es el número de identificación de la VLAN.

Las VLANs se implementan mediante: la asociación de un puerto a una VLAN, denominada VLANs por puerto; y por la asociación de la dirección MAC del dispositivo a una VLAN, conocidas como VLANs por MAC. Dependiendo de su función, se definen diferentes grupos de VLANs, por ejemplo VLANs: de datos, de voz, nativa, de administración y predeterminada.

1.1.5 CABLEADO ESTRUCTURADO ^{[5][6]}

Toda red se apoya en la infraestructura y los elementos que permiten la interconexión de los sistemas informáticos y de comunicación. Sin importar que tan sofisticados sean los equipos, si fallan los medios que los interconectan, éstos no podrán trabajar correctamente.

Se ha demostrado que la mayoría de inconvenientes reportados al trabajar con redes se debe a problemas con los elementos de interconexión, tales como cables defectuosos o a inadecuadas técnicas de instalación.

Un sistema de cableado estructurado se define como una única red de cableado dentro de un edificio que conecta los diferentes dispositivos de comunicación y permite la interconexión con redes externas. En las normas y estándares de cableado estructurado se especifica qué elementos usar en la interconexión, cómo instalarlos, cómo administrarlos y cómo probarlos para obtener el mejor desempeño de la red.

1.1.5.1 Estándares de Cableado Estructurado ^{[5][6]}

La Alianza de Industrias Electrónicas (EIA, *Electronic Industries Alliance*) en conjunto con la Asociación de Industrias de Telecomunicaciones (TIA, *Telecommunications Industry Association*) definen las principales normas y estándares para cableado estructurado.

Para sistemas de cableado estructurado, dentro de oficinas o instalaciones de uso comercial, se tienen las siguientes normas:

- EIA/TIA 568-B.1,2,3. Conjunto de normas que describe qué elementos usar y cómo instalarlos en sistemas de telecomunicaciones para instalaciones comerciales, haciendo uso de par trenzado y fibra óptica.
- EIA/TIA 569-B. Describe los recorridos y espacios de telecomunicaciones para instalaciones comerciales. En él se definen 6 subsistemas de cableado:
 1. Acometida. Es el punto dentro del edificio donde se interconectan los servicios cableados o inalámbricos externos.
 2. Cuarto de Equipos. Espacio reservado para la concentración de equipos de telecomunicaciones, tales como servidores.
 3. Cuarto de Telecomunicaciones. Terminación de los puntos del cableado horizontal. También sirve como punto de conexión hacia el cableado vertical.
 4. Cableado Vertical (*Backbone*). Cableado que interconecta al cuarto de equipos, cuartos de telecomunicaciones y entradas de servicios.
 5. Cableado Horizontal. Cableado que se extiende desde el cuarto de telecomunicaciones hasta el área de trabajo.
 6. Área de Trabajo. Es el espacio dentro de un edificio donde los usuarios interactúan con computadores, impresoras y dispositivos en general.
- EIA/TIA 606. Provee un esquema de administración uniforme e independiente de las aplicaciones.

1.1.5.2 Categorías de Cable para Cableado Estructurado ^{[5][6]}

El medio de transmisión más difundido en instalaciones dentro de edificios por su relación entre costo y confiabilidad es el cable de par trenzado. De éste existen algunas variantes, de las cuales la más utilizada es el par trenzado sin blindaje (cable UTP, *Unshielded Twisted Pair*).

El cable de par trenzado inicialmente se utilizaba en instalaciones de Telefonía Analógica, luego fue mejorado para cubrir los requerimientos de las redes de datos. Cada mejora introducida especifica una nueva categoría de cable con un mayor rango de frecuencias de operación. En la tabla 1.1 se detallan las categorías de par trenzado UTP.

Categoría	Frecuencia de Operación [MHz]	Distancia [m]	Observaciones
Cat 3	4	100	Puede usarse en sistemas de Telefonía Analógica.
Cat 5e	100	100	Es el cable más utilizado en instalaciones comerciales, oficinas y residencias; recomendable para sistemas <i>Fast Ethernet</i> .
Cat 6	250	100	Es la última categoría aceptada y reconocida dentro de los estándares de cableado estructurado.

Tabla 1.1 *Características de las categorías de cable UTP*

En las nuevas categorías se está reemplazando el cable UTP por cables con algún tipo de blindaje, que soportan mayores rangos de frecuencia, como por ejemplo los cables: STP (*Shielded Twisted Pair*), ScTP (*Screened UTP*) y FTP (*Foiled Twisted Pair*).

1.1.6 REDES WAN

Las redes WAN nacen de la necesidad de interconectar redes LAN distribuidas geográficamente y cubrir mayores distancias. Su objetivo sigue siendo la compartición de sus recursos e información. A diferencia de las LAN donde se usa infraestructura propia de una organización para la conexión, en una WAN se

utilizan los servicios de operadores o *carriers*, lo cual resulta más económico que implementar una WAN para cada organización.

1.1.6.1 Tecnologías WAN ^[7]

Para la conexión de redes en distintos lugares, las tecnologías utilizan técnicas de conmutación, que pueden ser de circuitos o paquetes.

- Conmutación de circuitos. Se establece un circuito o canal dedicado de extremo a extremo. Existirá un establecimiento de conexión, transmisión de información y una finalización de conexión.
- Conmutación de paquetes. La información es fragmentada en paquetes de tamaño variable los que se transmiten por un canal compartido. No existe la necesidad de establecer y finalizar una conexión.

La conmutación de circuitos es una tecnología que principalmente se utiliza en Telefonía tradicional. En las redes WAN organizacionales se utilizan tecnologías WAN de conmutación de paquetes. Entre las más utilizadas están: Frame-Relay, ATM (*Asynchronous Transfer Mode*), MPLS (*MultiProtocol Label Switching*).

1.1.6.1.1 *Frame-Relay* ^{[7][8]}

Es una tecnología que opera en las capa Física y Enlace del modelo de referencia OSI. El protocolo de capa Enlace se encarga de encapsular los paquetes que llegan de la capa Red en tramas de diferente tamaño, transportándolas a través de un único enlace compartido. El enlace o canal de transmisión puede ser punto a punto o punto multipunto, siendo su conexión lógica y utilizando circuitos virtuales. Los circuitos virtuales pueden establecerse dinámicamente, llamándose circuitos virtuales conmutados (*SVC, Switched Virtual Circuit*), o pueden ser preconfigurados, los cuales se conocen como circuitos virtuales permanentes (*PVC, Permanent Virtual Circuit*). Para su establecimiento, los circuitos virtuales Frame-Relay utilizan las direcciones DLCI (*Data Link Connection Identifier*) que tienen significado a nivel local.

1.1.6.1.2 ATM (*Asynchronous Transfer Mode*)^{[7][8]}

Permite el transporte de voz, video y datos a través de su red. A diferencia de Frame-Relay, encapsula la información de capas superiores en tramas de longitud fija llamadas celdas. El tamaño fijo de una celda es de 53 bytes, 48 bytes de datos y 5 bytes de cabecera. ATM mantiene el esquema de circuitos virtuales e incluye los conceptos de canales virtuales (VC, *Virtual Channel*) y caminos virtuales (VP, *Virtual Path*). Los canales virtuales son los enlaces que se establecen para la transmisión. Los caminos virtuales se establecen entre *switches* ATM y pueden contener varios canales virtuales.

1.1.6.1.3 MPLS (*MultiProtocol Label Switching*)^{[8][36][37]}

Es un protocolo sencillo que se ubica entre las capas Enlace y Red del modelo de referencia OSI. Fue desarrollado para el fácil manejo de tráfico de datos, voz y video. MPLS añade una cabecera a los paquetes de la capa Red. Esta cabecera puede contener una o más etiquetas, las mismas que sirven para definir el tipo de servicio y facilitar el enrutamiento entre dispositivos intermedios. MPLS trabaja independientemente de los protocolos disponibles en las capas de Enlace y de Red. Tiene características especiales de diseño para las áreas de: QoS (*Quality of Service*), Ingeniería de Tráfico, Redes Privadas Virtuales (VPNs) y Soporte Multiprotocolo.

1.1.7 EQUIPOS DE CONECTIVIDAD

Los equipos de conectividad más importantes que se encuentran en una red de datos son: *hubs*, *bridges*, *switches*, *routers* y *gateways*.

Las funciones de los equipos de conectividad pueden ser implementadas directamente en *hardware* como equipos dedicados, o también pueden ser desarrollados en *software* en equipos de propósito general.

1.1.7.1 *Hub* ^{[2][3][38]}

Conocido también como concentrador, trabaja en la capa Física del modelo OSI. Es un equipo que interconecta varios dispositivos en un mismo segmento de red. El *hub* puede ser del tipo pasivo, si únicamente deja pasar la señal; o del tipo activo, si éste amplifica la señal que por él pasa, llamado también repetidor.

Entre las características más importantes de un *hub Ethernet* se encuentran el soporte de las velocidades de 10 y 100 Mbps y el número de puertos. El número de puerto es determinante en el rendimiento de una red. A mayor número de puertos existirá mayor probabilidad de colisiones provocando la saturación del medio compartido. Comúnmente la cantidad de puertos en un *hub* es de: 4, 6, 8, 12, 16 y 24.

1.1.7.2 *Bridge* ^{[2][4]}

El *bridge* es un equipo que trabaja en la capa 2 del modelo OSI. Permite la interconexión de dos segmentos de red de similares o distintas tecnologías LAN, usando las direcciones físicas MAC de destino. A diferencia de un *hub*, el *bridge* tiene cierta inteligencia que le permite filtrar las tramas y retransmitirlas al otro segmento únicamente cuando sea necesario.

1.1.7.3 *Switch* ^{[2][3][4]}

El conmutador o *switch*, es un equipo que trabaja principalmente en la capa 2 del modelo OSI, pero puede hacerlo también en las capas 3 y 4. Permite la conexión de dos o más estaciones o segmentos de red. Su función principal es conmutar las tramas recibidas por un puerto enviándolas a otro. Utiliza la tabla de direcciones MAC donde se encuentra la asociación entre un dispositivo y el puerto al que está conectado para conmutarlo correctamente. Realiza además la división de la red en múltiples dominios de colisión.

Los *switches* de capa 3 además de cumplir las funciones principales de conmutación, realizan funciones de enrutamiento, mediante la utilización de protocolos para este fin. Así mismo permiten la interconexión entre diferentes dominios de *broadcast*.

Los *switches* de capa 4 además de realizar funciones de un *switch* de capa 3, pueden realizar funciones de NAT¹ (*Network Address Translation*), establecer políticas y filtrar la información que es manejada por la capa 4.

1.1.7.4 Router ^[4]

Es un equipo que trabaja en la capa Red del modelo OSI y enruta paquetes entre redes de diferente tecnología. Para enrutar los paquetes entre redes distintas, un *router* toma la dirección de red y dependiendo de su destino envía el paquete por la mejor ruta disponible. A diferencia de un *switch*, el *router* es un equipo con mayor inteligencia, que permite realizar un control y filtrado usando información de la capa Red. Esto hace que el equipo requiera mejores características de procesamiento incrementando su complejidad en relación a la de un *switch*.

1.1.7.5 Gateway ^{[14][15]}

Los *gateways* son dispositivos que regularmente se ubican en el borde de una red para conectarse con otras. El mundo de las redes es heterogéneo en cuanto a las tecnologías y protocolos que se utilizan, por ello los *gateways* se encargan de traducir los protocolos que cumplen similares funciones pero tienen capacidades diferentes.

1.1.8 ARQUITECTURA TCP/IP ^{[1][3][4]}

Además del modelo ISO/OSI, existen otros modelos que sirven de referencia en el mundo de las redes. Uno de ellos es el modelo TCP/IP, que ha posibilitado el gran despliegue del Internet. Nace como creación del Departamento de Defensa de los

¹ NAT es un mecanismo usado por *routers* IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. (ANÓNIMO. Wikipedia: http://es.wikipedia.org/wiki/Network_Address_Translation)

Estados Unidos, como la red ARPANET. A diferencia del modelo ISO/OSI que sólo define las funciones de las capas, en el modelo TCP/IP también se indica su implementación mediante un *stack* de protocolos bien definido. Esta característica le otorga la denominación de arquitectura.

La arquitectura TCP/IP se encuentra dividida en 4 capas comparables con el modelo OSI. La figura 1.4 muestra los dos modelos: ISO/OSI y TCP/IP.

Como se puede apreciar en la figura 1.4, las 4 capas del modelo TCP/IP son: *Host-Red*, Internet, Transporte y Aplicación.

La capa *Host-Red* equivale a las capas Física y Enlace del modelo ISO/OSI. No define un medio de transmisión específico, por lo que el modelo TCP/IP se adapta a cualquier medio físico de transmisión posible.

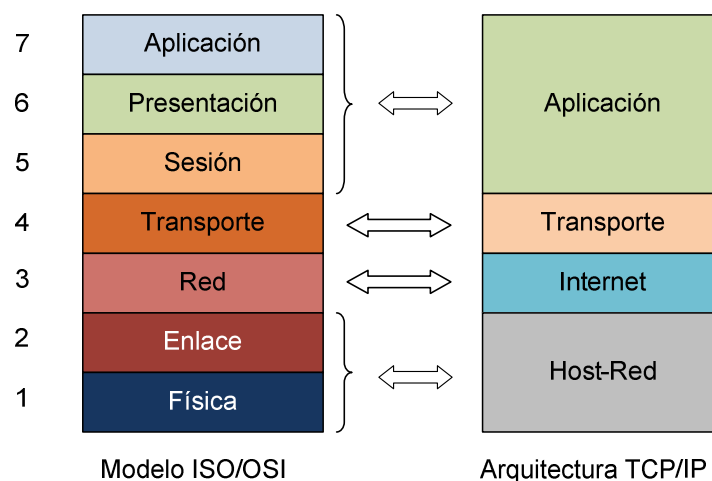


Figura 1.4 *Relación entre las capas del modelo ISO/OSI y de la arquitectura TCP/IP*

La capa Internet es la responsable de dividir los datos provenientes de las capas superiores en paquetes y enviarlos a través de la red hacia su destino. Cada paquete viaja independientemente de los demás y puede llegar en un orden diferente del enviado. De ser requerido, las capas superiores reordenan los paquetes. Esto contrasta con la capa Red del modelo OSI, puesto que se descarta el servicio de transmisión confiable a este nivel. El protocolo definido para esta capa es el protocolo IP (*Internet Protocol*).

La capa Transporte es la que permite a dos dispositivos, origen y destino, establecer una conversación a través de diferentes redes. Dos protocolos están definidos en esta capa: TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*), descritos más adelante.

La capa Aplicación contiene los protocolos de alto nivel con los cuales el usuario interactúa directamente. Las funciones de las capas Sesión y Presentación se incluyen en esta capa en caso de necesitarse.

Al igual que en el modelo ISO/OSI, en cada capa del modelo TCP/IP se realiza el proceso de encapsulamiento de los datos. Esta tarea es realizada por un protocolo específico en cada capa, definiendo Unidades de Datos de Protocolo (*PDU, Protocol Data Unit*).

1.1.8.1 Protocolo IP ^{[3][4]}

El Protocolo Internet, o IP, es el principal protocolo usado para proveer entrega de paquetes en redes TCP/IP, siendo la base de la conmutación de paquetes. Fue diseñado como un protocolo no orientado a conexión, tolerante a fallos y enrutable a través de diferentes redes. Es conocido como el protocolo del mejor esfuerzo por dejar a las capas superiores la resolución de errores.

La unidad de datos del protocolo IP es el paquete. En la figura 1.5 se muestra la estructura de un paquete IPv4.

En la cabecera del paquete IPv4 existen campos relacionados con la versión del protocolo IP, la longitud del paquete, tipo de paquete y las direcciones de origen y destino. En la actualidad existen dos versiones del protocolo IP, la versión 4 y la versión 6, siendo la primera la más difundida y utilizada. La versión 6 se crea en respuesta a las necesidades de direcciones IP de mayor longitud y mejoras en la seguridad.

El campo Tipo de Servicio (*TOS, Type of Service*) está relacionado con la clasificación de los datos que transporta. Este campo permite dar un trato especial a cada paquete de forma independiente.

1.1.8.1.1 Direccionamiento IP ^{[3][4]}

Las direcciones IP origen y destino posibilitan la entrega inequívoca de cada paquete a su destinatario. Las direcciones IPv4 constan de 32 bits, divididos en 4 octetos para su interpretación decimal.

Existen 3 grandes clases de direcciones IP: A, B y C, que se discriminan por la cantidad de estaciones o *hosts* que admite una red. En cada clase se tiene un rango de direcciones para uso privado.

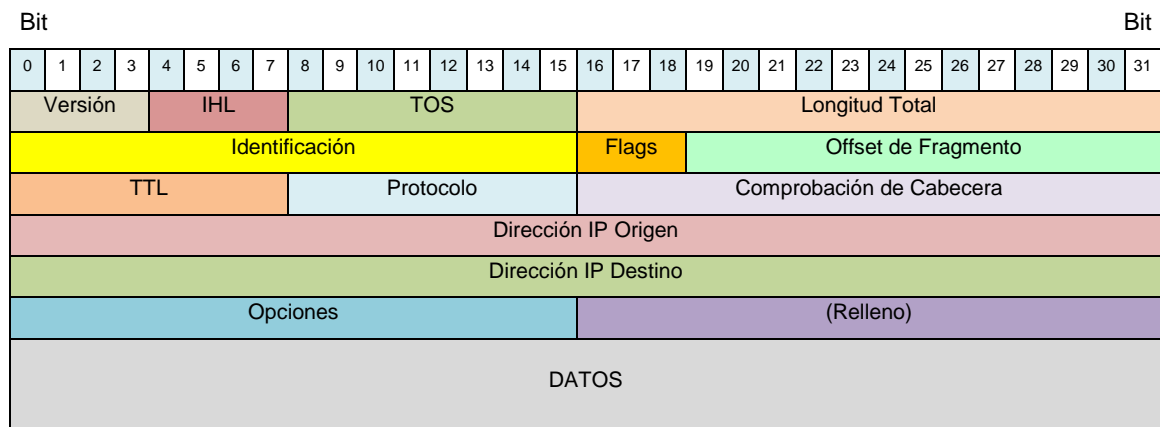


Figura 1.5 Estructura del paquete IPv4

Además de las direcciones IP, se tiene un parámetro también de 32 bits denominado máscara. La máscara permite hacer sub-agrupaciones de direcciones para limitar el número de *hosts* que forman una subred.

1.1.8.2 Protocolos TCP Y UDP ^{[1][3][4]}

Los protocolos TCP (*Transmission Control Protocol*) y UDP (*User Datagram Protocol*) prestan servicios de transporte de datos a la capa aplicación al tiempo que hacen transparentes los detalles de funcionamiento del protocolo IP. Múltiples

aplicaciones de un *host* pueden hacer uso de los servicios de red mediante TCP o UDP según se requiera, identificadas por un número de puerto único.

TCP brinda un transporte confiable y orientado a conexión. La confiabilidad de TCP reside en la confirmación de llegada de cada mensaje al emisor; si existiese algún error, se lo notifica y se pide la retransmisión del mensaje. Una comunicación TCP implica establecimiento de conexión, transmisión de mensajes y liberación de la conexión.

UDP por otra parte, ofrece un servicio no confiable y sin conexión.

1.1.9 MODELO CLIENTE – SERVIDOR Y APLICACIONES DE RED ^{[3][4][8]}

El modelo cliente-servidor define la interacción entre un proceso llamado cliente y otro llamado servidor. El cliente realiza una petición al servidor en espera de una respuesta. Una estación puede tener varios procesos simultáneos con el rol de cliente o servidor, pudiéndose tener múltiples sesiones de este tipo con otras estaciones. Cuando estaciones con las mismas capacidades intercambian los roles de cliente y servidor, se les denomina pares. La mayoría de aplicaciones de red se basan en el modelo cliente-servidor para su funcionamiento (figura 1.6).

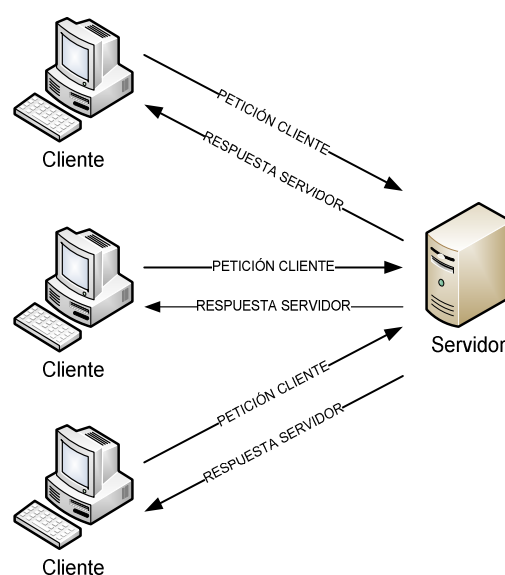


Figura 1.6 *Funcionamiento del modelo Cliente - Servidor*

Diferentes aplicaciones surgieron de la necesidad de compartir recursos en la red, diferenciándose una de otra por el servicio que entrega al usuario final. Cada aplicación está implementada en base a protocolos de alto nivel tales como: HTTP (*Hypertext Transfer Protocol*) para navegación web, FTP (*File Transfer Protocol*) para compartición de archivos, SMTP (*Simple Mail Transfer Protocol*) para correo electrónico, SNMP (*Simple Network Management Protocol*) para monitorizar y gestionar redes remotamente, NTP (*Network Time Protocol*) para sincronización de tiempo, NNTP (*Network News Transfer Protocol*) como servicio de noticias, etc.

1.2 TELEFONÍA TRADICIONAL

La invención del teléfono posibilitó la transmisión de la voz por medio de señales eléctricas a través de un cable. A medida que fueron dándose a conocer los beneficios de poder comunicarse con cualquier persona, prácticamente sin importar la distancia, un mayor número de individuos demandó el acceso a este servicio. Desde entonces la Telefonía se convirtió en el sistema que permitía a usuarios de todo el mundo comunicarse entre sí.

Los primeros sistemas de Telefonía solucionaron el problema de la demanda masiva a este servicio. Lo hicieron a través de sistemas cableados diseñados para cubrir capacidades y necesidades diferentes. Con el avance de la tecnología, pasando de la Telefonía Analógica a digital, se mejoraron las técnicas de conmutación. La señalización se introdujo para el establecimiento y control de las llamadas.

1.2.1 SISTEMAS TELEFÓNICOS TRADICIONALES

En un inicio, el servicio de Telefonía se brindaba mediante la instalación de líneas punto a punto entre los usuarios. El incremento en el número de usuarios determinó la concentración de las líneas telefónicas en una oficina central para interconectar múltiples usuarios, reduciendo la cantidad de recursos necesarios.

Existen dos sistemas telefónicos tradicionales de uso en la actualidad: la red telefónica pública conmutada (*PSTN, Public Switched Telephone Network*) y las centrales telefónicas privadas (*PBX, Private Branch eXchange*). Estos sistemas son similares a las redes LAN y WAN, por el área de servicio que cubren.

1.2.1.1 PSTN (*Public Switched Telephone Network*) ^{[9][10][39]}

La Red Telefónica Pública Conmutada, o PSTN, es una red que conecta terminales telefónicos fijos entre sí a nivel mundial. Hace uso de la conmutación de circuitos para brindar servicios de Telefonía en tiempo real.

La PSTN, simbolizada en la figura 1.7, está compuesta de una serie de centrales telefónicas que operan en diferentes localidades, agrupando y dando servicio a cierto número de usuarios. Las centrales se encargan de establecer los circuitos o caminos temporales para que los usuarios puedan comunicarse.

Del lado del usuario está el teléfono que cumple con la función de CPE (*Customer Premise Equipment*) o equipo terminal de usuario, mediante el cual se accede a los servicios de la PSTN. Tradicionalmente, la conexión entre el usuario y la central se realiza a través de pares de cobre; a este enlace se lo denomina última milla.

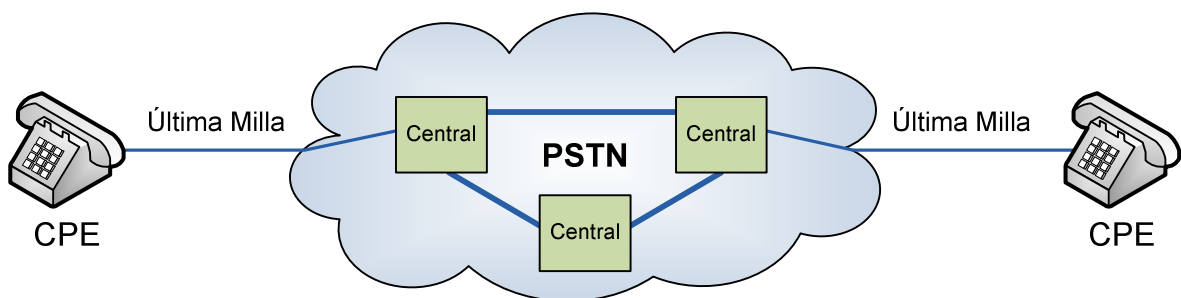


Figura 1.7 Representación del sistema telefónico de la PSTN

Los servicios e infraestructura de la PSTN son provistos por un proveedor u operador. Los usuarios deben arrendar al operador las líneas telefónicas según sus necesidades. Bajo este esquema, el usuario se denomina abonado.

1.2.1.2 PBX (*Private Branch eXchange*) ^{[9][10][39]}

Para un número reducido de usuarios es factible arrendar al proveedor una a una las líneas necesarias para acceder a la PSTN. Sin embargo, para un número considerable de usuarios que requieren principalmente realizar llamadas entre sí dentro de la misma ubicación, arrendar todas esas líneas resulta ineficiente y costoso.

Una PBX es un sistema telefónico autónomo que permite dar servicios varios de Telefonía a usuarios en un área determinada. Las PBXs son pequeñas centrales telefónicas que conmutan las conexiones de sus usuarios y permiten la interconexión con otras PBXs y hacia la PSTN. La PSTN se conecta hacia una PBX con un grupo de líneas telefónicas denominadas troncales. Las troncales contienen un número de líneas, que es independiente de la cantidad de usuarios que pueda manejar la PBX; el número de troncales suele ser menor, para así ahorrar recursos. Las PBX son de uso privado, por lo general forman parte de la infraestructura del edificio y su operación es transparente para la PSTN.

1.2.2 CONMUTACIÓN DE CIRCUITOS ^{[9][10][30][31]}

La conmutación en los inicios de la Telefonía se realizaba manualmente. Una operadora era la encargada de conectar las llamadas a sus destinos. Para facilitar el trabajo de conexión de abonados, en sus contratos de servicio se les asignaba un número identificativo de su línea o número telefónico. La limitación de las operadoras llevó a que se desarrollen métodos de conmutación más eficientes para la conexión de los usuarios.

La conmutación electromecánica fue el siguiente camino tomado por el sistema telefónico. Su principal característica era el uso de dispositivos mecánicos que permitían conmutar una llamada, conocidos como selectores y buscadores. Luego se integró el relé como mecanismo de selección y dio inicio a la conmutación semielectrónica. El avance de la tecnología en el campo de la computación generó la combinación de relés y el computador en el sistema telefónico. El uso

del computador como equipo de procesamiento desarrolló la digitalización de la voz, permitiendo que se almacenen las señales digitales de los circuitos de entrada en memoria para luego ser leídos en orden diferente, dando lugar a la multiplexación en el tiempo. En la multiplexación espacial a diferencia de la temporal, las señales combinan sus líneas múltiples de entrada y salida pero conservan el mismo estado de tiempo.

1.2.3 TELEFONÍA ANALÓGICA Y DIGITAL ^{[9][10]}

En Telefonía se realizan dos operaciones fundamentales: la transmisión de la voz y el control asociado a esa transmisión. La Electrónica marcó la diferencia en el tratamiento y transmisión de las señales de voz. Así se pasó de sistemas telefónicos analógicos a sistemas telefónicos digitales.

Los sistemas telefónicos analógicos empezaron con el establecimiento de circuitos eléctricos para la transmisión de la voz entre dos usuarios. Consistían principalmente de dos circuitos entre el usuario y la central, uno para las señales de voz y otro para señales relacionadas con el control.

Posteriormente, se introduce la multiplexación por división de frecuencia (*FDM, Frequency Division Multiplexing*). Este método consiste en introducir varias señales de diferente frecuencia en un mismo medio de transmisión, sin que se interfieran. Así se lograba transportar varias conversaciones telefónicas por el mismo canal.

En el mundo de las telecomunicaciones se prefieren las señales digitales a las analógicas. Esto se debe a que la señal original transmitida puede ser recuperada del lado del receptor de forma íntegra. Las señales digitales pueden ser representadas con estados lógicos, unos y ceros (1's y 0's), denominados bits. De esta forma las conversaciones telefónicas y las señales de control pueden compartir un mismo medio de transmisión, siendo identificadas y discriminadas por una secuencia específica de bits. En Telefonía Digital se usa la multiplexación por división de tiempo (*TDM, Time Division Multiplexing*). En TDM se toman

muestras de varias señales de voz digitalizada y se las intercala en ranuras de tiempo. Un ejemplo de red de Telefonía Digital es la red digital de servicios integrados (*RDSI*).

1.2.4 ETAPAS DE UNA LLAMADA TELEFÓNICA ^{[9][11]}

En un sistema telefónico una llamada realizada satisfactoriamente pasa por las siguientes etapas:

1. Envío del número marcado. Los terminales telefónicos son identificados mediante una dirección numérica. El teléfono llamante le envía a la central el número con el cual se desea contactar.
2. Conexión de los teléfonos. La central verifica el número recibido y determina el teléfono al cual se pide la conexión. En este instante la central establece un camino entre el teléfono llamante y el teléfono llamado.
3. Timbrado en el teléfono llamado. La central notifica al teléfono llamado de una llamada entrante mediante una señal de timbrado.
4. Contestación de la llamada. El usuario inicia la conversación al levantar el auricular.
5. Conversación. Intercambio de información entre los usuarios llamante y llamado.
6. Finalización de la llamada. La llamada puede ser finalizada tanto por el usuario que realiza la llamada como por el usuario que la recibe, basta con colgar el auricular. Así se envía una señal de liberación de la conexión a la central.

1.2.5 SEÑALIZACIÓN ^{[9][10][11]}

La señalización se define como el intercambio de información específicamente relacionada con: el establecimiento de conexiones entre terminales telefónicos, monitoreo de la conexión mientras está en uso y liberación de la conexión cuando finaliza la llamada. Estas etapas y procesos se realizan sin que el usuario esté pendiente de los detalles de funcionamiento, siendo transparentes para él.

Las señales pueden ser agrupadas según las funciones que éstas realizan: supervisión, direccionamiento, alerta y progreso de la llamada.

- Supervisión. Se trata de monitorear la línea o circuito para saber si está ocupado, libre o requiriendo un servicio.
- Direccionamiento. Es el proceso de transmitir señales de ruta y destino a través de la red.
- Alerta. Consiste en avisar al llamado de una llamada entrante. Estas alertas pueden ser visuales o audibles.
- Progreso de la llamada. Son señales que informan al usuario del estatus de la llamada, por ejemplo si la línea está ocupada o se está realizando el marcado.

La señalización también ha ido cambiando con la tecnología. En los primeros sistemas telefónicos la señalización dependía del *hardware* subyacente, tal como en DTMF (*Dual Tone Multi-Frequency*). Otros sistemas de señalización como SS7 (*Signaling System 7*) hacen uso de tecnología digital, independizando la señalización del *hardware*.

1.2.6 SERVICIOS ^[54]

Con la integración del computador al sistema telefónico se pudo hacer uso de la gran capacidad de procesamiento y de memoria, para permitir nuevos servicios a más de la transmisión de voz. Estos servicios son activados según las necesidades de los usuarios. Dependiendo del sistema, sea la PSTN o una PBX, se tienen los siguientes servicios:

- **Servicios especiales.** Números reservados para llamadas a servicios de emergencia, por ejemplo: 100 - Información CNT, 101 - Policía, 102 - Bomberos, 103 - Cruz Roja, entre otros.
- **Servicios suplementarios.** Son servicios que requieren una activación previa. Para ello el usuario debe ser categorizado en el instante en que se suscribe al servicio. Los servicios complementarios realizan únicamente la función para la cual están programados; son limitados, se activan y desactivan desde el aparato telefónico. Ejemplos: llamada en espera,

transferencia de llamadas, línea conmutada directa, candado electrónico, rastreo de llamadas, buzón de mensajes, reloj despertador, entre otros.

- **Servicios de red inteligente.** Son servicios que no forman parte de la central telefónica en la PSTN, sino que residen en el lado del usuario que contrata el servicio, pero el operador se encarga de activarlos. El usuario para acceder al servicio debe marcar un código conjuntamente con un número de identificación personal y otros códigos adicionales dependiendo del servicio. La red inteligente posibilita la creación de nuevos servicios usando *hardware* y *software*. Ejemplos: 1-700, 1-800, 1-900. El servicio de 1-800 o *Advanced Freephone Service* es un servicio que se accede desde cualquier teléfono y permite al usuario realizar llamadas gratuitas. La tarificación del servicio se la realiza al número que recibe la llamada.

1.2.7 LIMITACIONES DE LA TELEFONÍA TRADICIONAL ^{[9][11][13]}

En los sistemas de Telefonía tradicional (analógicos o digitales) la capacidad es proporcional a las conexiones físicas que manejan. Mientras más usuarios se añadan al sistema, más equipos y tarjetas deberán ser añadidos. Usualmente cuando llegan al límite de capacidad, es necesario migrar a otros equipos, mientras los primeros quedan inutilizados. Esto significa cambiar los esquemas de diseño y modificar el espacio físico. Por ende, los sistemas telefónicos tradicionales crecen lentamente y las actualizaciones son costosas.

Otro problema es la falta de estandarización entre los equipos y terminales telefónicos. Por ejemplo, la mayor parte de PBXs son propietarias. Éstas sólo interactúan con otras PBXs y terminales de la misma marca. Incluso se tiene incompatibilidad con los servicios y funciones entre diferentes modelos del mismo fabricante.

Si bien las redes de Telefonía tradicional han cumplido con el objetivo de transportar la voz con una calidad que satisface al usuario, los servicios adicionales que ofrecen cambian lentamente y son costosos de implementar. Las redes de datos por otra parte, gracias al desarrollo del *software*, se caracterizan

por su escalabilidad y rápida evolución de servicios sin mayores cambios en el *hardware*.

1.3 TELEFONÍA IP

Los dos primeros pasos que se dieron antes de formar el concepto de Telefonía IP fueron la digitalización de la voz y la Voz por IP o VoIP. Éstas fueron dos técnicas usadas en la etapa de transición de distintos sistemas de comunicaciones, dados los beneficios de las comunicaciones digitales.

1.3.1 DIGITALIZACIÓN DE LA VOZ Y CÓDECS DE AUDIO ^{[9][11][40]}

El proceso de conversión de análogo a digital de una señal se lleva a cabo mediante un códec, acrónimo de codificador/decodificador. El algoritmo más conocido para digitalizar señales de voz, por su uso en redes digitales de Telefonía, es el de Modulación por Codificación de Pulsos, PCM (*Pulse Code Modulation*). En PCM se establecen 3 etapas: muestreo, cuantización y codificación.

- Muestreo. Se trata de definir intervalos de tiempo en el cual se toman muestras de la señal. El oído humano no detecta las variaciones instantáneas presentes en las señales de voz, por lo que no es necesario tomar muestras contiguas. El intervalo tomado en PCM es de 125 us, suficiente para señales de voz y tolerable para el oído humano.
- Cuantización. Se definen los valores o niveles de amplitud que la señal puede tomar. Cada muestra es aproximada al valor establecido más cercano durante el intervalo de muestreo. PCM establece 256 niveles de cuantización.
- Codificación. A cada nivel se le identifica con un valor binario, de manera que éste no se repita. A cada uno de los 256 niveles se los puede identificar con 8 bits. Al final del proceso se obtiene una secuencia de unos y ceros que representan al audio digitalizado. La velocidad de transmisión resultante de esta señal es de 64 kbps.

Para poder reproducir el audio digitalizado, en el decodificador se siguen los mismos pasos en orden inverso.

Debido a las etapas de muestreo y cuantización, la señal digitalizada pierde algunas de sus características lo que se percibe como una disminución en la calidad de la señal audible. Es posible mejorar esta situación reduciendo el intervalo de muestreo y aumentando el número de niveles de cuantización, con lo que se incrementa la velocidad de transmisión de la señal resultante. Por desgracia, existen enlaces con capacidad limitada; por lo que transportar señales de alta velocidad por estos medios, generalmente compartidos, no es la mejor opción.

La ITU y otros organismos han estandarizado varios códecs basados o no en PCM, diseñados para reducir la velocidad de transmisión y mejorar la calidad auditiva de la señal. Para determinar cuál de ellos presenta la mejor calidad auditiva se introduce el concepto de MOS (*Mean Opinion Score*). El MOS es una calificación numérica subjetiva, debida a la percepción auditiva de las personas cuando se utilizan diferentes codecs. La tabla 1.2 contiene las características de los principales codecs usados para transmisión de voz.

Codificador	Estándar/ Recomendación	Velocidad de Transmisión	MOS	Retardo Codificador/ Decodificador
PCM	G.711	64 kbit/s	4.1	125 μ s
ADPCM	G.726	32 kbit/s	3.85	300 μ s
RPE-LTP	ETSI – GSM 06-10	13 kbit/s	3.6	50 ms
CELP	DD FS1016	4.8 kbit/s	3.5	50 ms
LC-CELP	G.728	16 kbit/s	3.61	3 ms
CS-ACELP	G.729	8 kbit/s	3.92	30 ms
MP-MLQ-ACELP	G.723.1	6.3 y 5.3 kbit/s	3.9 y 3.8	90 ms
LCP	DOD LPC10 FS1015	2.4 kbit/s	2.3	50 ms

Tabla 1.2 *Características de códecs para la transmisión de voz*

Como se puede apreciar, cada códec tiene características distintas que pueden ser deseables o no dependiendo de la aplicación.

1.3.1.1 VoIP, Voz sobre IP ^{[13][20]}

La posibilidad de comunicarse desde cualquier parte del mundo, a través de Internet, así como la digitalización de la voz, hicieron atractivo el transporte de las conversaciones telefónicas sobre las redes de datos con un costo mínimo. Mientras en la PSTN cada llamada tiene un costo variable según el tiempo que dura, los enlaces de datos son cotizados por su capacidad a un precio fijo en un periodo de tiempo, por ejemplo mensual.

VoIP o voz sobre IP, es una tecnología en la cual una aplicación de usuario realiza el proceso de digitalización de la voz y la transmite a través de una red IP. VoIP a diferencia de la Telefonía tradicional se maneja sobre conmutación de paquetes, mejorando la utilización de los canales de comunicación. Los paquetes se construyen con la voz digitalizada, que se encapsula dentro de los protocolos de la arquitectura TCP/IP.

Internet trabaja en su mayoría con TCP/IP, lo que facilita la comunicación mundial de la voz por esta red. Existen aplicaciones, gratuitas y licenciadas, que permiten hacer llamadas gratuitas a través de Internet utilizando VoIP; entre las principales se encuentran: Skype, Windows Live Messenger, Open Wengo, Ekiga, Tapioca.

VoIP tiene ciertas limitaciones relacionadas con el retardo y la pérdida de paquetes que afectan la calidad de la voz. Éstos se producen por la utilización de una red que no fue creada para manejar comunicaciones a tiempo real. Al necesitar la voz un tratamiento especial se incrementan nuevos protocolos y estándares para mejorar su transmisión en las redes de datos. Con esto se pretende prestar mejores servicios a los encontrados en la Telefonía tradicional, con calidad similar. Así se genera el concepto de Telefonía IP.

1.3.1.2 Características de Telefonía IP ^{[11][12][13][14]}

Telefonía IP es un término utilizado para describir un conjunto de productos y soluciones, basados en el protocolo IP como mecanismo de transporte, convirtiendo a una red de datos en una red convergente, capaz de brindar servicios de voz, video y datos.

La Telefonía IP presenta varias ventajas sobre la Telefonía tradicional, como son: el diseño de aplicaciones según las necesidades del usuario, la simplificación de la administración, el ahorro en rubros relacionados con telecomunicaciones; además, introduce el concepto de las comunicaciones unificadas, como la forma en que se integran los servicios de comunicación.

Para que las redes de datos soporten aplicaciones y servicios en tiempo real, como se requiere en Telefonía IP, aparecen principalmente dos estándares: SIP y H.323. Estos estándares introducen sus propios protocolos que junto a TCP/IP y otros estándares controlan las comunicaciones y resuelven los problemas de calidad de servicio encontrados en las redes de datos. SIP y H.323 cumplen con las funciones de señalización presentes en la Telefonía tradicional.

Una de las claves de la rápida inserción y evolución de las redes de datos en el mundo, es que están basadas fuertemente en estándares. Organismos internacionales como la IETF (*Internet Engineering Task Force*), la ITU (*International Telecommunications Union*), la ISO o la IEEE han definido las normas y procedimientos para que los equipos de comunicaciones de diferentes fabricantes puedan operar entre sí.

Dos estándares de Telefonía IP han tenido un fuerte desarrollo y aparecen como opciones viables para su implementación: H.323 y SIP. Cada uno de ellos cuenta con su propia arquitectura, las cuales pueden ser utilizadas para el establecimiento de comunicaciones multimedia con calidad de servicio.

1.3.2 RECOMENDACIÓN H.323 ^{[14][41][42]}

H.323 es una recomendación propuesta por la ITU-T (*International Telecommunications Union-Telecommunications*), que especifica los protocolos a ser utilizados para la comunicación multimedia en redes basadas en paquetes IP. La creación de H.323 tenía por objetivos: basarse en estándares previos para la integración con distintos sistemas vigentes, aprovechar las ventajas de usar una red de conmutación de paquetes y facilitar el envío de información en tiempo real a través de dicha red.

1.3.2.1 Arquitectura H.323 ^[14]

La arquitectura H.323 necesita para su funcionamiento de los elementos que se muestran en la figura 1.8.

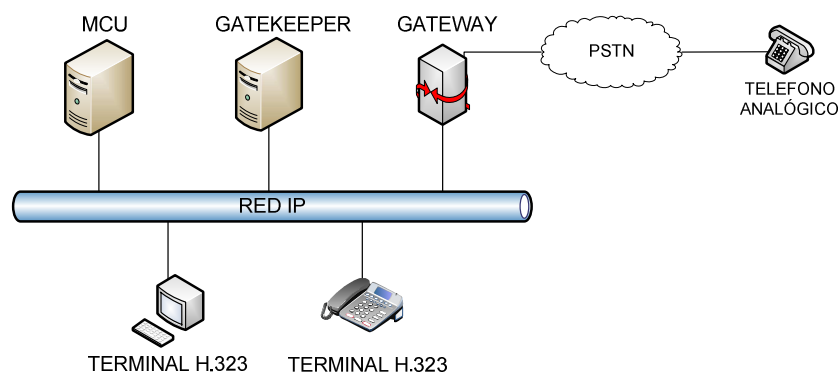


Figura 1.8 Componentes de la Arquitectura H.323

- **Terminal.** Es un dispositivo de comunicación que se encuentra al alcance del usuario final. Permite la interacción del usuario con la aplicación. Éstos pueden ser PCs con su respectivo *software* y *hardware* multimedia, terminales telefónicos específicos, teléfonos multimedia 3G, PDA (*Personal Digit Assistant*), entre otros.
- **Gateway.** Permite la interconexión entre H.323 y una red conmutada de circuitos; convierte los protocolos de señalización y los formatos de los medios de comunicación (figura 1.9). Pueden existir PSTN/voice *Gateway*, PSTN/fax *Gateway*, GSM *Gateway*, PBX *Gateway*, entre otros.

- **Multipoint Control Units (MCUs).** Permiten realizar conferencias entre 3 o más terminales; usualmente contiene un controlador multi-punto, que está encargado del control y señalización de la conferencia, y un procesador multi-punto para el procesamiento de la información enviada por los terminales.
- **Gatekeeper.** Es el administrador de un grupo de dispositivos H.323 que conforman una zona. Realiza las funciones de traslación de direcciones, control de ancho de banda² mínimo, control de admisión de terminales y administración de una zona. El *gatekeeper* es opcional pero con su implementación se logra un mayor rendimiento. Puede estar implementado en una PC o integrado al *Gateway*.

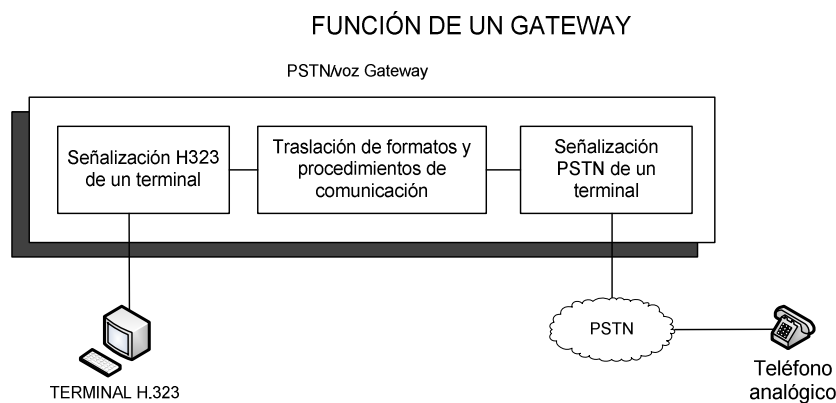


Figura 1.9 *Funcionamiento de un gateway de voz*

1.3.2.2 Protocolos H.323 ^{[14][41]}

Las funcionalidades de las comunicaciones se especifican a través del uso de protocolos que forman el *stack* de protocolos H.323. La mayoría de estos protocolos ya están siendo utilizados actualmente en redes y otros aún no se han implementado. Todos los protocolos de H.323 están ubicados sobre la capa Transporte por lo que permite cualquier tipo de tecnología en la capa Física y Enlace.

² Ancho de Banda es referenciado como la velocidad de transmisión, que representa la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

- **H.225.0-Q.931.** Protocolo que proporciona los procedimientos de señalización entre dos terminales. Es responsable de la creación y liberación de una llamada. Está basado en la recomendación Q.931 de redes ISDN por lo que facilita la interconexión con redes de este tipo.
- **H.245.** Permite realizar el control multimedia entre dos terminales, es decir posibilita el intercambio de información de las capacidades multimedia que tienen los terminales para establecer una comunicación. Las llamadas se posibilitan solo si ambos terminales tienen las mismas capacidades.
- **H.225-RAS (*Registration Admissions and Status*).** Realiza los procesos de registro, admisión, estatus y brinda la señalización para la conexión entre un terminal y un *gatekeeper*. El terminal accede a servicios que puede ofrecer un *gatekeeper*, como: autenticación AAA y resolución de direcciones.
- **H.450.** Este protocolo brinda la señalización entre dos dispositivos inteligentes H.323, además proporciona servicios complementarios de H.323.
- **H.235.** Protocolo que proporciona seguridad mediante autenticación o cifrado de los terminales.
- **RTP (*Real-Time Transport Protocol*) Y RTCP (*Real-Time Transport Control Protocol*).** Son protocolos utilizados por la arquitectura H.323, pero creados por el IETF, para el control y transmisión de comunicaciones en tiempo real.

1.3.2.3 Establecimiento de una Llamada H.323 ^{[14][41]}

El proceso de una llamada telefónica IP es similar al que se tiene en Telefonía tradicional. En H.323 ciertos protocolos permiten iniciar y terminar una llamada, así como el control que se tenga de la misma. Es importante identificar los dispositivos que van a intervenir en el proceso ya que de esto dependerá uno u otro modelo de señalización. Los modelos de señalización típicos para el establecimiento de una llamada en H.323 dependerán del *gatekeeper*. El *gatekeeper* es el único que decide el tipo de señalización. Cuando distintos protocolos y mensajes pasan a través de él, se trata de una *señalización enrutada*

a través del *gatekeeper*. Cuando distintos protocolos y mensajes se intercambian directamente entre los dos terminales a conectar, se trata de una *señalización directa*, en la cual no interviene el *gatekeeper*.

Para el establecimiento de una llamada utilizando una señalización enrutada a través del *gatekeeper*, se cumple el siguiente proceso (figura 1.10).

- 1. Descubrimiento y registro con el *Gatekeeper*.** El terminal envía un mensaje de *multicast* para identificar a su *gatekeeper* y éste lo responde con un paquete de confirmación. El terminal se registra enviando su dirección y alias y finalmente el *gatekeeper* confirma su registro.
- 2. Configuración de la llamada mediante la señalización H.225.0-Q.931.** El terminal envía información de los parámetros de la llamada al *gatekeeper* y éste enruta dicha información al otro terminal a conectar. Si este terminal acepta los parámetros procederá a registrarse con el *gatekeeper*. Si el *gatekeeper* acepta la llamada, enviará información del canal de control de llamada H.245 para el intercambio de capacidades.
- 3. Inicio de la comunicación e intercambio de las capacidades.** Los terminales a conectar intercambian mensajes con la información de las capacidades multimedia que éstos tienen, como son los códecs de audio y video. Si los terminales son compatibles para una comunicación multimedia se podrán abrir los canales respectivos para la comunicación.
- 4. Establecimiento de la comunicación multimedia y control de la misma.** Los terminales intercambian información sobre el canal lógico multimedia por el cual van a transmitir. La información multimedia se enviará por un canal usando el protocolo de transporte UDP, mientras que la información de control se enviará usando el protocolo de transporte TCP.

Para el establecimiento de una llamada con señalización directa se cumple el mismo procedimiento anterior, con la diferencia de que no es necesario el descubrimiento y registro con el *gatekeeper*. El intercambio de información de los parámetros para el establecimiento de la llamada se los realiza directamente con el terminal a conectar (figura 1.11).

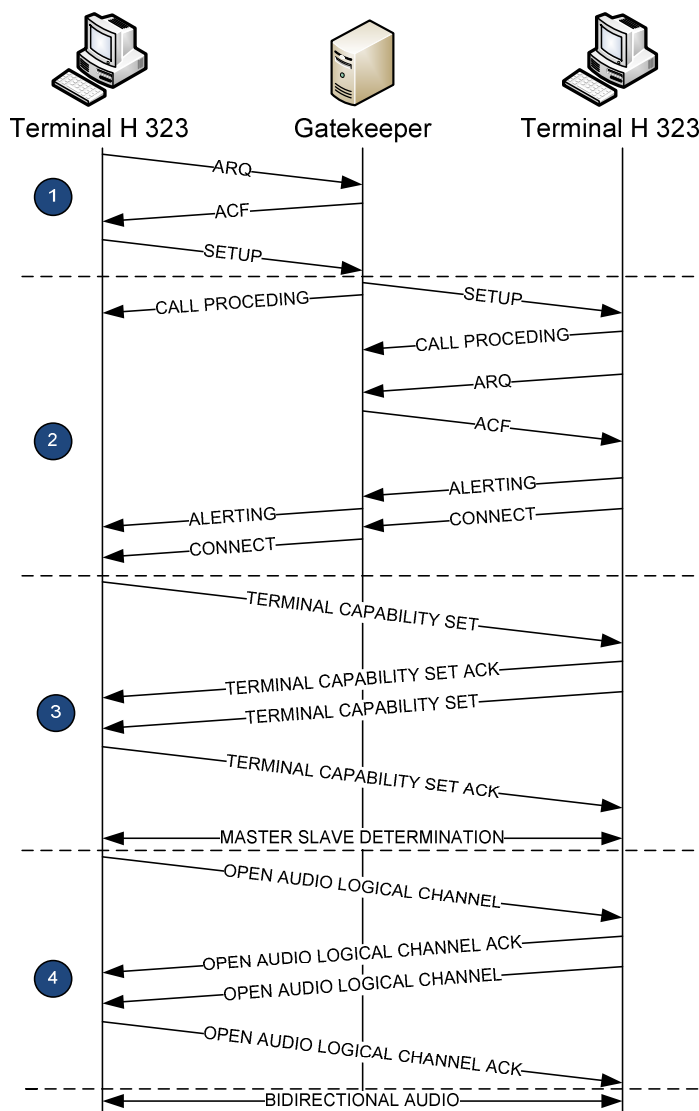


Figura 1.10 *Establecimiento de una llamada H.323 con señalización enrutada por el gatekeeper*

1.3.2.4 Terminación de una Llamada H.323 ^{[14][41]}

La terminación de una llamada puede ser realizada por cualquiera de los dos terminales. El terminal que decida finalizar la llamada debe cumplir con el siguiente procedimiento:

- Se realizará la petición de cierre de los canales lógicos de comunicación abiertos. Se recibe una confirmación de la misma.

- Se envía la petición de cierre de los canales de control H.245. Se recibe su correspondiente confirmación.

Finalmente se envía un mensaje de *RELEASE COMPLETE* entre ambos terminales por medio de H.225.0-Q.931. Si se trata de una señalización enrutada a través del *gatekeeper* se liberan los registros mediante mensajes del protocolo H.225.0-RAS.

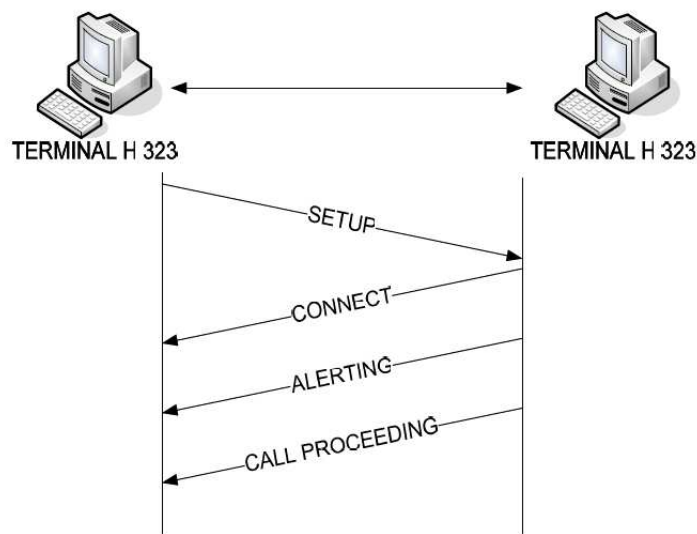


Figura 1.11 *Establecimiento de una llamada directa sin gatekeeper*

1.3.3 SIP (*Session Initiation Protocol*) ^{[15][18][46]}

Más y más aplicaciones en el Internet habilitan a los usuarios a comunicarse entre sí de una u otra forma. Mensajería instantánea, videoconferencias, juegos interactivos y otras aplicaciones multimedia necesitan mecanismos para invitar a otros usuarios a participar. El protocolo de inicio de sesiones SIP fue desarrollado para establecer, mantener y terminar sesiones interactivas entre terminales de usuario.

SIP es el protocolo principal dentro del conjunto de protocolos de la arquitectura que lleva su mismo nombre. El IETF continúa el desarrollo de SIP cuya versión actual es la número 2, estandarizada en el RFC 3261. Este estándar tiene como

mira las comunicaciones en la Internet por lo que reutiliza funciones y características ya implementadas, como el enrutamiento y el direccionamiento, o el formato de mensajes encontrados en HTTP y SMTP.

1.3.3.1 Funciones de SIP ^{[17][18]}

SIP fue diseñado para cubrir las siguientes cinco características específicas del establecimiento de sesiones:

- **Ubicación de usuario.** Debido a que el usuario puede hacer uso de distintos dispositivos para conectarse a una red, esta función de SIP ayuda a determinar cuál de ellos está siendo utilizado.
- **Disponibilidad de usuario.** Estados de presencia como: conectado, ausente u ocupado ayudan a los participantes a iniciar sesiones de forma más eficiente.
- **Capacidades de usuario.** SIP está orientado a soportar sesiones independientemente del medio, por lo tanto la sesión se establece en base a capacidades que sean comunes entre los terminales.
- **Configuración de la sesión.** Los parámetros se negocian y se establece la sesión.
- **Gestión de la sesión.** Durante una sesión los parámetros pueden cambiar. Es posible que se inviten a nuevos participantes, se cambie el estatus de presencia o de la llamada, se cambie el dispositivo de comunicación, etc.

1.3.3.2 Arquitectura SIP ^{[15][16][17][18]}

Para su funcionamiento SIP utiliza cuatro tipos de entidades: Agentes de Usuario, Servidores Registrar, Servidores Proxy y Servidores de Redirección. Estos elementos intercambian mensajes cuyo contenido y características son empaquetados mediante el protocolo SDP (*Session Description Protocol*) para completar la sesión.

Entidades SIP:

- **Agentes de Usuario:** Son los dispositivos terminales de usuario, tales como teléfonos celulares, computadores, PDAs, etc. utilizados para crear y manejar sesiones SIP. El agente cliente UAC (*User Agent Client*) envía un mensaje y el agente servidor UAS (*User Agent Server*) responde a este mensaje. Para la conexión con redes que no son SIP, es el *gateway* el que se comporta como agente.
- **Servidor Registrar:** Contiene las bases de datos con la información de ubicación de todos los agentes de usuario que se han registrado dentro de un dominio. Este servidor recoge las direcciones IP y otra información de los participantes que comparte con el servidor Proxy.
- **Servidor Proxy:** Acepta las invitaciones de sesión de los agentes de usuario y consulta al servidor Registrar la dirección del agente destinatario. Entonces reenvía la invitación de sesión directamente al agente destinatario si se encuentra en el mismo dominio, caso contrario a otro servidor Proxy. El servidor Proxy puede también ofrecer servicios como: control de acceso a la red, seguridad, autorización y autenticación.
- **Servidor de Redirección:** Se emplea por SIP para redireccionar a los clientes hacia los agentes con los que se quieren contactar. Cuando un agente hace una petición al servidor de Redirección éste le puede responder con la dirección IP del agente a ser contactado. La diferencia con el servidor Proxy es que el servidor de Redirección sólo responde a una petición, no reenvía invitaciones de sesión. Otra función del servidor de Redirección es “timbrar” a todas las posibles ubicaciones de un usuario al que se desee llamar. La sesión se establece en la primera ubicación donde se conteste la llamada y se liberan los demás destinos.

De los elementos descritos, los 3 tipos de servidores pueden ser implementados en conjunto en el mismo *hardware*. En el caso de los agentes, es común que sean implementados independientemente, como los teléfonos habilitados con SIP o *software* telefónico para el computador (*softphones*).

1.3.3.3 SDP (*Session Description Protocol*) ^{[15][16][17][46]}

El principal protocolo utilizado en conjunto con SIP para establecer las sesiones es el protocolo SDP. SDP describe las características de los dispositivos terminales, así como las capacidades multimedia.

Los mensajes SDP se encapsulan dentro de mensajes SIP y son utilizados cuando se necesita establecer comunicaciones en tiempo real, como audio y video. La cabecera de un mensaje SDP contiene un descriptor que identifica las especificaciones de la sesión. Mediante los descriptores es posible identificar el nombre de la sesión, su propósito, el tiempo de inicio, qué medios son empleados para la sesión (códecs), las direcciones y puertos a ser utilizados para recibir los medios. Los medios aceptados incluyen: audio, video, aplicación, datos y control.

1.3.3.4 Establecimiento de Sesiones SIP ^{[15][16]}

La figura 1.12 representa una sesión SIP simple que se establece entre dos dispositivos terminales habilitados con SIP, conectados a una red de paquetes.

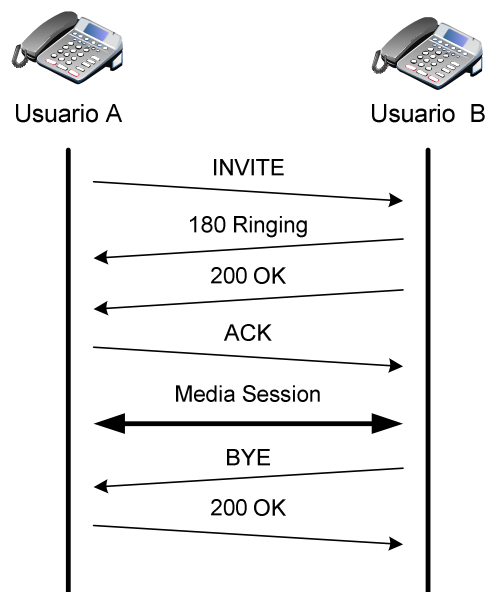


Figura 1.12 *Establecimiento de una sesión SIP simple entre dos terminales*

Asumiendo que cada dispositivo terminal conoce la dirección del otro:

1. El usuario A invita al usuario B a iniciar una sesión con un mensaje *INVITE*. El mensaje *INVITE* contiene los detalles del tipo de sesión o llamada que se requiere. Puede ser una simple sesión de voz o algo más avanzado como una videoconferencia.
2. El usuario B indica al usuario A que se está alertando de la invitación, mediante un mensaje 180 *RINGING*. Éste es un mensaje de información para el cual no se necesita respuesta.
3. Cuando el usuario B acepta la llamada, se envía un mensaje 200 *OK* que también indica que el tipo de medio propuesto por el usuario A es aceptable para la llamada.
4. Entonces el usuario A envía un mensaje de confirmación para empezar el intercambio de medios.
5. La conversación multimedia en el caso de Telefonía IP, se lleva a cabo a través del protocolo RTP.
6. Cualquiera de los dos participantes puede dar por concluida la llamada con un mensaje *BYE*, enviado en este caso por el usuario B.
7. La confirmación al cierre de sesión es provisto por el usuario A con un mensaje 200 *OK*.

En el ejemplo anterior, se ha supuesto que los terminales tienen la información suficiente para establecer una sesión entre ellos. Sin embargo, en un dominio con múltiples agentes es necesario introducir a los servidores Registrar, Proxy y Redirección para obtener la información de contacto y poder establecer la comunicación.

1.3.3.4.1 Registro SIP^[17]

Antes de que un agente pueda iniciar una comunicación con otro cliente, cada participante debe estar registrado con un servidor Registrar. Para esto, el agente envía un mensaje *REGISTER* al servidor SIP como se muestra en la figura 1.13. Una vez que la petición ha sido aceptada, las direcciones SIP e IP son añadidas al servicio de localización.

1.3.3.4.2 Rol del Servidor Proxy^[17]

Por medio del servidor Proxy, el agente A realiza una invitación de sesión al agente B. El servidor Proxy chequea la información de ubicación con el servidor de Registro (figura 1.14) para determinar la dirección IP del agente solicitado. El agente B se contacta al servidor Proxy y, a través de éste, envía la respuesta al agente A. En caso de una respuesta afirmativa, la conversación puede iniciar.

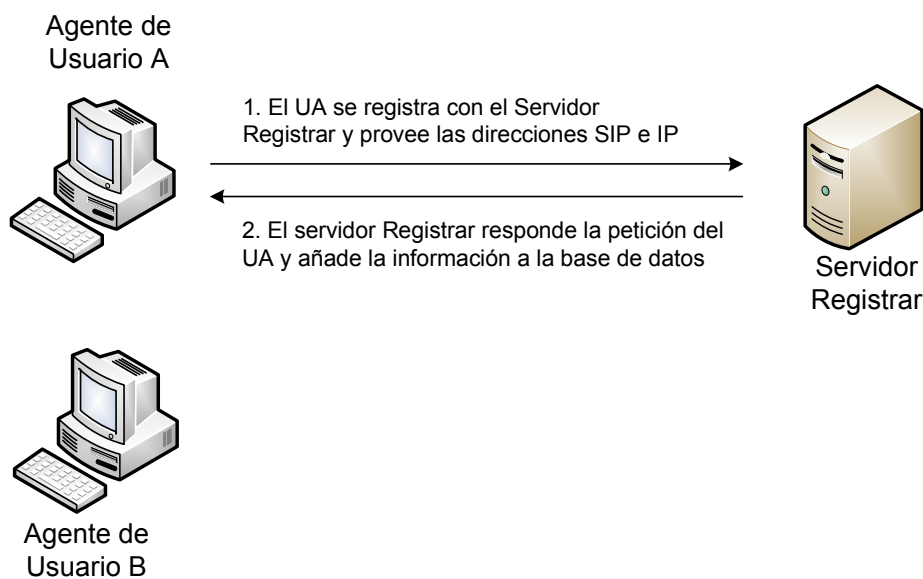


Figura 1.13 Registro de un Agente de Usuario con el Servidor Registrar

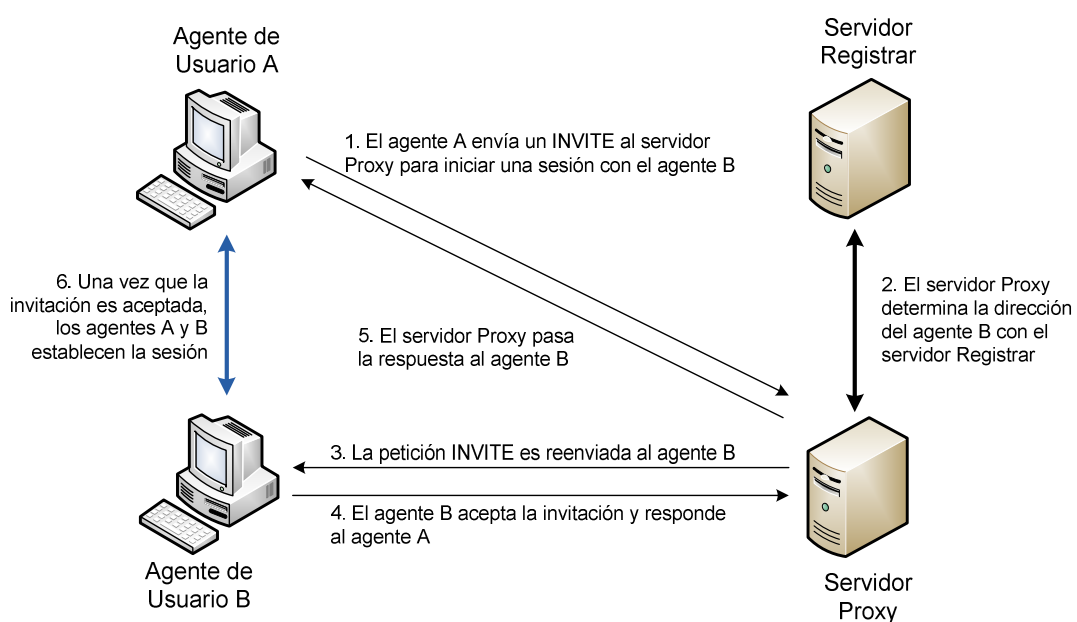


Figura 1.14 Establecimiento de una sesión SIP mediante el servidor Proxy

1.3.3.4.3 Rol del Servidor de Redirección ^[17]

Al estar presente el servidor de Redirección (figura 1.15), el agente A le pide directamente a él la ubicación del agente B. El servidor de Redirección consulta la información de localización con el servidor de registro. Una vez que el agente A obtiene la dirección de B, le envía directamente el mensaje *INVITE* y sigue el proceso de la figura 1.12.

Como se ha mencionado antes, SIP no se ocupa de todos los aspectos de una comunicación multimedia, por lo que es relativamente más simple que otras arquitecturas tales como H.323. Por ejemplo, SIP no provee por sí mismo calidad de servicio; para esto se apoya en protocolos como el protocolo de reserva de recursos (*RSVP, Resource Reservation Protocol*). El transporte de medios los puede hacer a través de RTP o SCTP (*Stream Control Transmission Protocol*), y los servicios complementarios son provistos por otros protocolos.

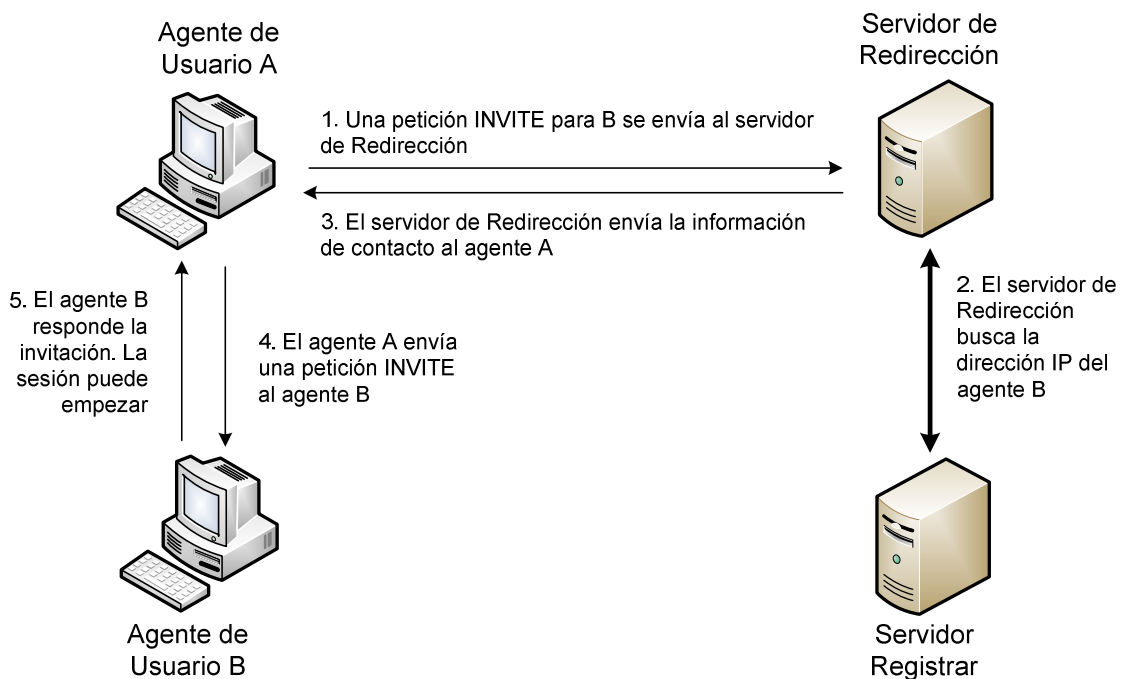


Figura 1.15 Establecimiento de una sesión SIP mediante el servidor de Redirección

1.3.4 COMPARACIÓN ENTRE SIP Y H.323 ^{[14][15]}

SIP y H.323 están diseñados esencialmente para cumplir las funciones de señalización en las comunicaciones multimedia. Trabajan en redes TCP/IP usando los servicios que sus protocolos proveen para el transporte de datos, calidad de servicio, encriptación, etc.

El conjunto de protocolos o *stack* de protocolos que forman las arquitecturas H.323 y SIP se muestran en las figuras 1.16 y 1.17.

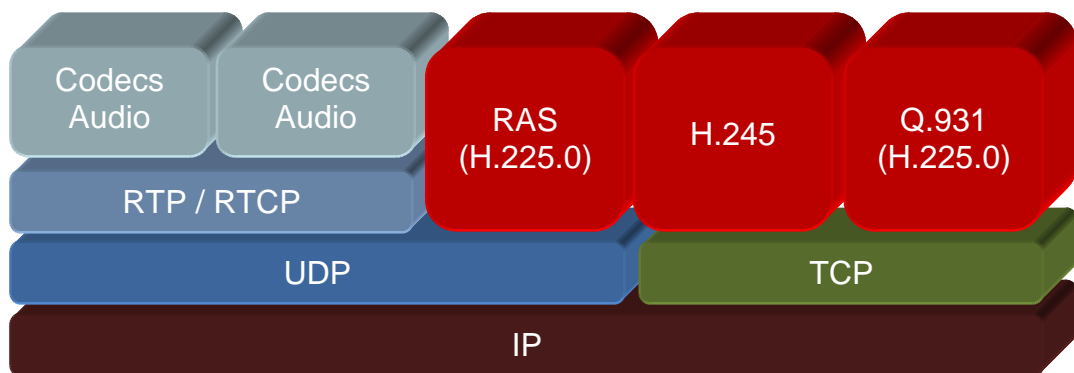


Figura 1.16 *Stack de protocolos H.323*



Figura 1.17 *Stack de protocolos SIP*

Las arquitecturas de SIP y H.323 tienen en común la necesidad de transportar la señalización y el audio/video (medios interactivos). Para la señalización en H.323 se usa TCP por sus características de confiabilidad. SIP por otro lado puede hacer uso de UDP, por su mejor rendimiento y escalabilidad; o TCP en el caso de que los mensajes de sesión necesiten fragmentación o una transmisión segura

con TLS (*Transport Layer Security*). SIP puede hacer uso de otros protocolos de transporte como SCTP (*Stream Control Transmission Protocol*).

1.3.5 PROTOCOLOS DE TRANSPORTE A TIEMPO REAL: RTP Y RTCP ^[14]

Las redes TCP/IP fueron creadas para transmisiones tolerantes a retardo y sin calidad de servicio. La voz necesita ser transmitida en secuencia, de forma confiable, a tiempo real y sin retardos excesivos. TCP es un protocolo confiable y que brinda secuenciamiento; pero estas características provocan retardos en las transmisiones, por lo que no podía ser utilizado en el transporte de la voz. UDP es un protocolo no confiable que no brinda secuenciamiento, pero a cambio no provocaba retardos. Al ser el retardo lo más crítico en una transmisión de voz se decidió que UDP provea el transporte. Para solucionar el nivel de confiabilidad y secuenciamiento se crearon protocolos como RTP y RTCP de manera que suplan esas falencias.

1.3.5.1 RTP (*Real-Time Transport Protocol*) ^{[8][17][43][44][46][47]}

RTP es un protocolo que permite el transporte de audio y video sobre el Internet definiendo un formato de trama estandarizado. RTP provee las funcionalidades de encapsulamiento de datos para transmisiones a tiempo real y funcionalidades para reconstruir los datos en su secuencia original. La encapsulación de RTP sólo puede ser vista por los dispositivos finales y no por los dispositivos intermedios ya que éste es un protocolo de capa Aplicación. RTP puede trabajar independientemente del protocolo que se encuentre en la capa Transporte. Además fue diseñado para trabajar con servicio de redes *unicast* o *multicast*.

Entre las funcionalidades que proporciona RTP se encuentran:

- **Número de secuencia.** UDP no transmite los paquetes con un número de secuencia, por lo que no se garantiza que los paquetes se reciban en el mismo orden en el que fueron enviados. Este número se utiliza para que

los paquetes tengan la secuencia correcta y para detectar los paquetes perdidos.

- **Timestamp.** Permite reproducir el *stream* de paquetes con la misma temporización con la que fue enviado.
- **Tipo de Payload.** Indica el tipo de codificación que se utilizó para los medios interactivos. La codificación se realiza mediante el uso de códecs que mejoran la utilización del ancho de banda y la calidad de la comunicación.

La cabecera de RTP contiene los bits necesarios para cumplir las funciones que intervienen en la transmisión de voz. En un mensaje RTP se encapsula la información de la voz que es digitalizada y codificada a través de códecs de audio más los bits de cabecera. El mensaje RTP se encapsula dentro de UDP/IP y del protocolo de la capa enlace que se encuentre. Para la recepción se realizará el proceso inverso, se quitarán las cabeceras de los protocolos que intervinieron en la comunicación hasta tener el mensaje RTP con la información de la voz. Esta información se almacena en un *buffer* de *jitter* dinámico para posteriormente ser decodificado y ser entregado al usuario (figura 1.18).

1.3.5.2 RTCP (RTP Control Protocol) ^{[43][45][47][48]}

Es un protocolo que trabaja conjuntamente con RTP recogiendo estadísticas de la calidad de la red por la cual se transmiten. El rendimiento de la red es importante para comunicaciones multimedia, por ello se transmiten estadísticas periódicas de *jitter*, número de paquetes enviados, número de paquetes recibidos, entre otros. Para una red con el estándar H.323 algunas funcionalidades de este protocolo se sobrepondrán a las proporcionadas por H.245. La diferencia de funcionalidades entre estos protocolos se podrá percibir en una red donde se necesite realizar conferencias con un número mayor a 1000 usuarios, en cuyo caso es necesario utilizar el protocolo RTCP; para pocos usuarios se usará el protocolo H.245. Esta distinción permite tener mejor rendimiento en una comunicación.

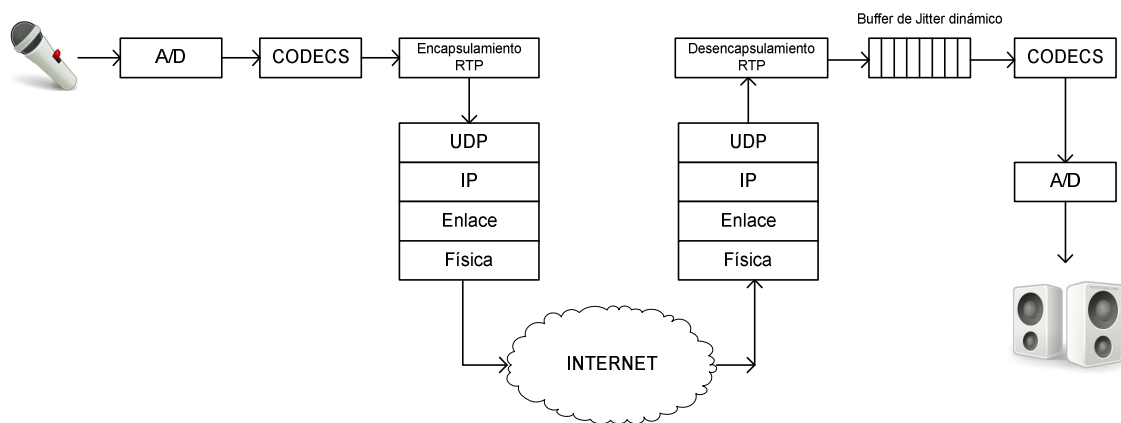


Figura 1.18 Funcionamiento de RTP

1.3.6 CALIDAD DE SERVICIO (QoS) EN REDES BASADAS EN IP ^{[19][20][21]}

En las redes de datos los paquetes llegan a su destino dándole poca importancia a la ruta, las veces que sean retransmitidos o el tiempo transcurrido. Esta característica no supe bien las necesidades para tráfico de aplicaciones interactivas o de tiempo real como una llamada telefónica. Si bien estas aplicaciones pueden soportar un ligero retraso (150 ms para la voz), es cuando se incrementan los niveles de pérdida de paquetes, de retraso y de variación en el retraso (*jitter*) que empiezan los problemas en la transmisión. La falta de calidad hace que el usuario se vea insatisfecho debido a que sus comunicaciones se retardan, se entrecortan o se distorsionan.

La calidad de servicio (*QoS, Quality of Service*) se puede definir como la capacidad de garantizar recursos y diferenciar servicios en una red de datos. Así se consigue que el tráfico producido por aplicaciones de distinta naturaleza pueda ser identificado y tratado adecuadamente para mejorar la experiencia del usuario.

En el caso de redes pequeñas como las LAN, que cuentan con una alta capacidad de transmisión y son parte del mismo dominio administrativo, es suficiente con determinar prioridades para el tráfico generado. Para diferenciar el tráfico de voz y datos, por ejemplo, se establece el uso de VLANs (802.1Q) o de priorización con 802.1p. Redes que escalan al nivel de Internet son más complejas. Es en ellas donde se presentan los principales problemas de calidad.

Para manejar calidad de servicio a nivel de Internet, el IETF ha desarrollado dos mecanismos: IntServ (*Integrated Services*) y DiffServ (*Differentiated Services*), que se apoyan en técnicas de encolamiento priorizado y tecnologías de transporte como MPLS.

1.3.6.1 IntServ (*Integrated Services*) ^{[19][22]}

IntServ o Servicios Integrados, es una estrategia para proveer reserva de recursos por flujo de *host-a-host* o *fin-a-fin*. Para obtener recursos garantizados, una aplicación debe hacer una reserva de recursos antes de que el tráfico comience a ser transmitido en la red. La reserva de recursos pasa por el siguiente proceso:

1. La aplicación debe caracterizar su fuente de tráfico y los requerimientos del recurso.
2. Se usa un protocolo de ruteo para encontrar un camino basado en los recursos requeridos.
3. Posteriormente, un protocolo de reserva se usa para indicar el estado de reserva a lo largo del camino.
4. En cada salto, el control de admisión chequea si existen suficientes recursos para el alojamiento.
5. Una vez que el camino se ha establecido, la aplicación puede comenzar a enviar su tráfico con el uso exclusivo de esos recursos.
6. La reserva de recursos se refuerza con la clasificación de los paquetes y mecanismos de planificación.

En IntServ se establecen tres modelos de servicio: garantizado, de carga controlada y del mejor esfuerzo.

- Servicio garantizado. Provee un servicio con retardo y velocidad de transmisión garantizados, basado en el peor de los casos.
- Servicio de Carga controlada. Es un servicio de menor garantía, en el cual se ofrecen condiciones similares a una red del mejor esfuerzo no cargada.
- Servicio del mejor esfuerzo. En él no se proveen garantías de ningún tipo.

IntServ cuenta con el protocolo de reserva de recursos RSVP (*Resource reSerVation Protocol*) para la señalización de QoS en cada salto.

1.3.6.1.1 RSVP (*Resource reSerVation Protocol*)^{[19][22][24]}

RSVP opera sobre IP ocupando el lugar de un protocolo de transporte según el modelo OSI. Sin embargo, RSVP no transporta ningún dato de aplicación. RSVP es principalmente un protocolo de señalización para reservar velocidad de transmisión dinámicamente y para tener un retardo uniforme garantizado en aplicaciones *unicast* o *multicast*. Es un protocolo de reserva unidireccional, con base en el receptor, para que las aplicaciones del emisor no monopolicen los recursos de la red. Si se desea una reserva en doble sentido, debe ser solicitada explícitamente por los extremos.

Los *routers* que se encuentran en el camino del flujo de datos realizan las peticiones de reserva si están habilitados con RSVP, los que no, simplemente dejan pasar los mensajes de reserva. A diferencia del establecimiento de circuitos virtuales, como en Frame Relay o ATM, los *routers* reservan los recursos al memorizar la información de estados (estados blandos). Cuando una ruta no se utiliza, los recursos son liberados. Si las rutas se cambian o modifican, los estados deben cambiar para mantenerse actualizados, por lo que se genera un tráfico periódico entre *routers*.

La reserva se realiza en dos pasos:

1. Las fuentes de información periódicamente generan mensajes de búsqueda de ruta para el camino con QoS, mediante algún protocolo de enrutamiento para comunicaciones *unicast* o alguna estructura de distribución *multicast*.
2. Los dispositivos receptores son informados de los requerimientos de reserva y responden mediante peticiones de reserva RESV, ejecutadas en los *routers*, siguiendo la ruta de regreso al emisor (figura 1.19).

La conexión lógica que se produce con RSVP se llama sesión y es descrita por 3 elementos:

- Dirección destino: Identifica al destino *unicast* o destinos *multicast*.
- Identificador de Protocolo: transporte TCP o UDP
- Puerto de Destino: TCP o UDP

RSVP provee calidad de servicio al controlar el tráfico, por medio de las siguientes funciones: control de admisión, clasificación de paquetes y planificación de paquetes. El control de admisión se basa en determinar qué peticiones de QoS pueden ser aceptadas. En la clasificación de paquetes, dependiendo de la información de la cabecera el paquete pasa a formar parte de una clase de servicio determinada. La planificación de paquetes consiste en reenviar los paquetes según la clase de servicio mediante mecanismos de priorización de encolamiento.

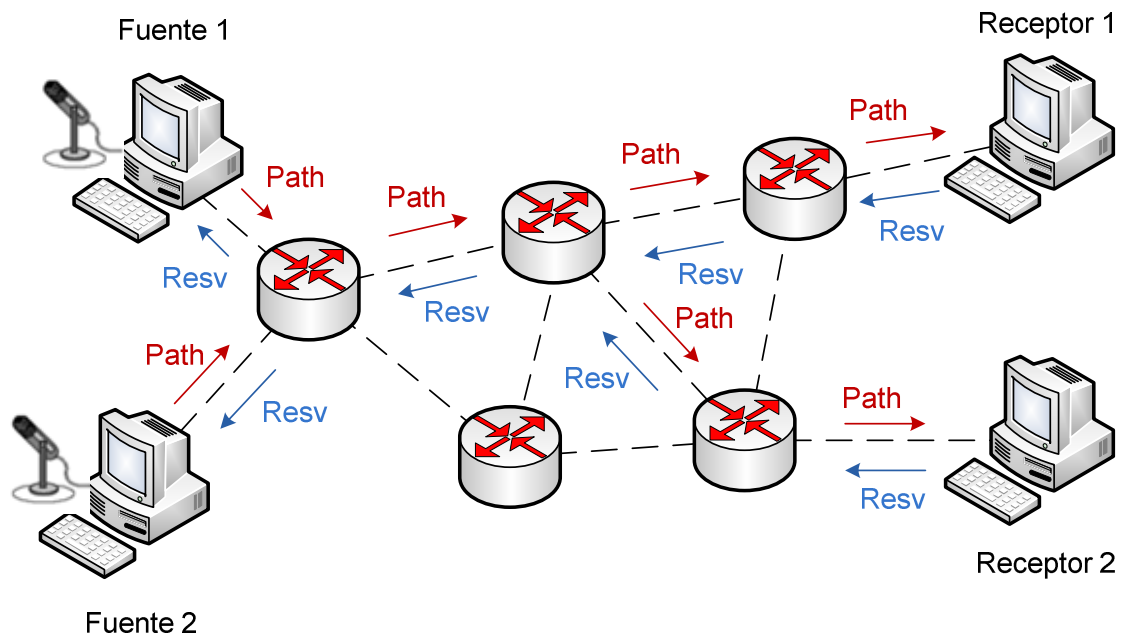


Figura 1.19 Proceso de Reserva RSVP

Implementar servicios integrados en Internet es complicado y poco práctico porque las reservas de caminos deben ser autorizadas, contabilizadas y autenticadas entre muchos proveedores de servicio y éstos deben ponerse de

acuerdo. En una red corporativa donde su tamaño es limitado y está bajo una sola administración esto es posible y recomendable.

1.3.6.2 DiffServ (*Differentiated Services*) ^{[19][22]}

Dados los problemas de escalabilidad de IntServ se desarrolló la estrategia de Servicios Diferenciados, DiffServ. A diferencia de IntServ que realiza la reserva de recursos por flujo a lo largo del camino, DiffServ realiza la diferenciación del tráfico en el borde de la red (figura 1.20) mediante políticas de borde, aprovisionamiento y priorización de tráfico.

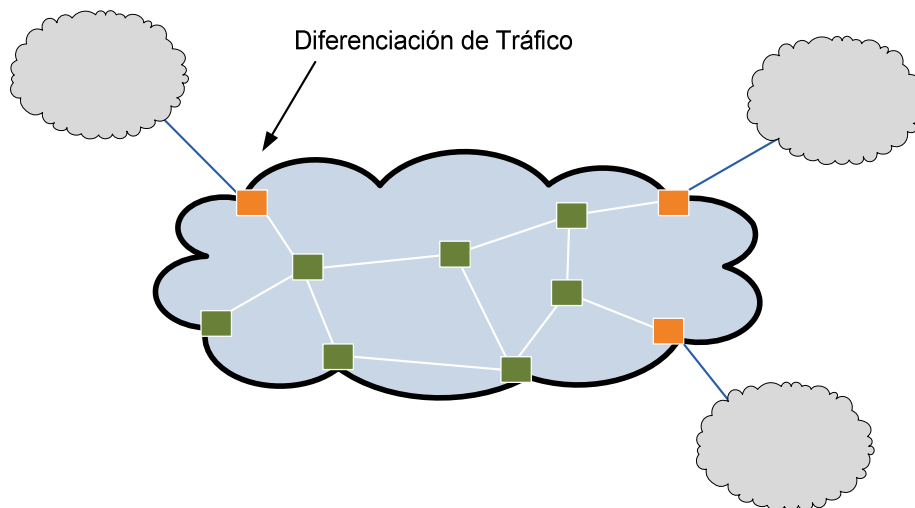


Figura 1.20 *Diferenciación de tráfico en el borde de la red con DiffServ*

En DiffServ el tráfico del usuario se divide en un pequeño número de clases de reenvío. Para cada clase de reenvío, la cantidad de tráfico que el usuario puede inyectar a la red es limitado en el borde de la red (WAN). Al cambiar la cantidad total de tráfico permitido en la red, el proveedor de servicio puede ajustar los niveles de aprovisionamiento de recursos y así dar un grado de garantía de recursos a los usuarios.

En la cabecera del paquete IP (campo tipo de servicio) se especifica la clase de reenvío. El borde de la red es responsable de asignar los paquetes a su respectiva clase de reenvío. Una vez que los paquetes han sido marcados en el borde, los nodos del interior de la red pueden usar esta información para

diferenciar el tratamiento de los paquetes. Las clases de reenvío pueden indicar si el paquete será descartado en caso de congestión o si tiene prioridad de reenvío.

Los servicios diferenciados escalan mejor que los servicios integrados. DiffServ no necesita el establecimiento de reserva de recursos. La asignación de las clases se especifican típicamente en los SLA³ y las clases se aplican al tráfico en conjunto y no a flujos individuales. Por otra parte, la complejidad de procesamiento se da en los bordes de la red donde el tráfico es mucho menor, lo que permite que el núcleo sea más simple.

En redes corporativas es factible tener una combinación de servicios integrados y diferenciados para aumentar la calidad de servicio fin-a-fin. IntServ se puede aplicar en la periferia de la red, en las redes de acceso, donde no presenta muchos problemas. DiffServ puede aplicarse en los bordes y el núcleo de la red. Este esquema se presenta en la figura 1.21.

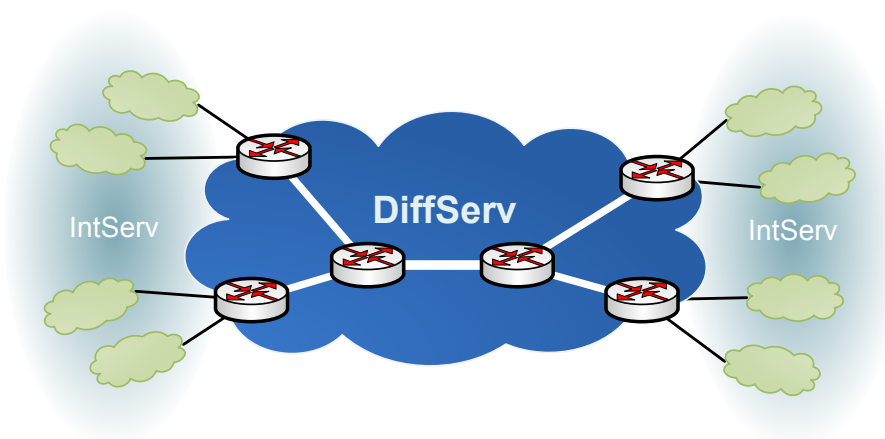


Figura 1.21 *Combinación entre DiffServ e IntServ*

1.3.6.3 Encolamiento Priorizado ^[20]

El comportamiento del mejor esfuerzo de IP implica que los paquetes que ingresan a un nodo se procesan en el orden de llegada, en un esquema FIFO (*First Input First Output*). Los paquetes que llegan más rápido de lo que el nodo

³ SLA (Service Level Agreement) o acuerdo de nivel de servicio, contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel de calidad de dicho servicio.

los procesa son almacenados en *buffers*. Una vez que éstos se llenan, los paquetes siguientes son descartados sin importar su naturaleza o procedencia.

Los esquemas de priorización indican a los dispositivos (*routers* o *switches*) cómo tratar a los paquetes en el momento de formación de las colas. Los dispositivos analizan los paquetes, determinan el tipo de tráfico que transportan, comparan esa información con una serie de reglas de priorización y utilización de ancho de banda para determinar el orden de salida de los paquetes.

Los esquemas más conocidos de encolamiento priorizado, de los cuales los fabricantes usan variantes o combinaciones son: colas de prioridad, colas del peso justo (*WFQ*, *Weight Fair Queuing*), y colas según la clase (*CBQ*, *Class-Based Queuing*).

1.3.6.3.1 Colas de Prioridad ^[20]

En este tipo de encolamiento, los paquetes son reenviados según una base estricta de prioridad. Los paquetes con la mayor prioridad son reenviados primero, luego los paquetes con el siguiente valor de prioridad, y así sucesivamente hasta llegar a la prioridad más baja (figura 1.22).

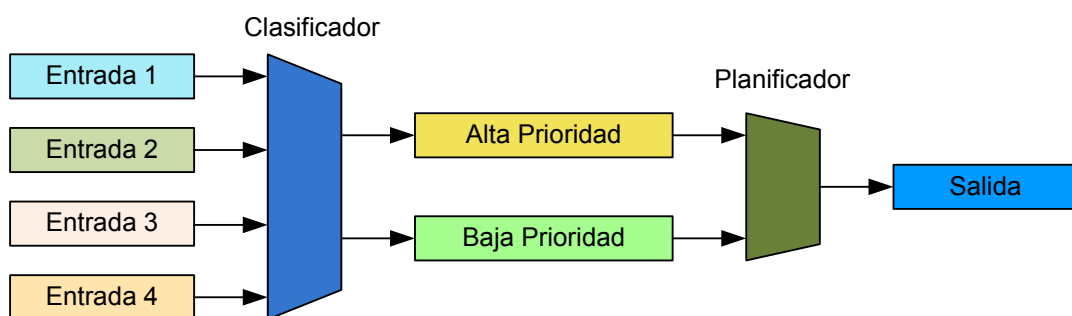


Figura 1.22 Diagrama de flujo de colas de priorización

Este mecanismo funciona bien para dar rendimiento altamente predictivo a los paquetes de alta prioridad. Sin embargo, los paquetes con prioridad baja podrían verse retrasados por largo tiempo si existe una gran cantidad de paquetes con prioridad alta. Las colas de prioridad funcionan mejor donde el tráfico de mayor

prioridad consumen un ancho de banda relativamente fijo (como el de la voz). Esto permite utilizar colas de prioridad mientras se sigue proporcionando un rendimiento predecible al tráfico de baja prioridad.

1.3.6.3.2 WFQ (Weighted Fair Queuing) ^[20]

WFQ o encolamiento según el peso, es un método diseñado para vencer los obstáculos de colas de prioridad. En WFQ se da una ponderación a los paquetes, basada en la prioridad y en el tiempo anticipado necesario para el procesamiento de esos paquetes (figura 1.23). Una vez que los paquetes tienen sus ponderaciones, salen según ese orden. Esto ayuda a seguir favoreciendo a los paquetes de alta prioridad, mientras se asignan recursos a otros paquetes de forma más justa.

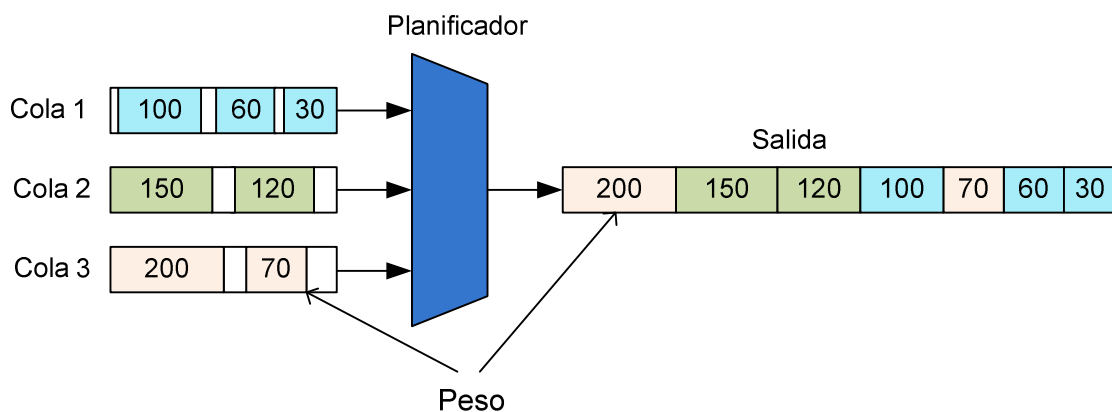


Figura 1.23 Diagrama de flujo de colas WFQ

WFQ tiene el inconveniente de ser un mecanismo bastante complejo y al ser implementado en *software* implica un retardo general para toda la transmisión.

1.3.6.3.3 CBQ (Class-Based Queuing) ^[20]

CBQ es una forma de cola en la que los paquetes se ordenan en clases según van llegando. Cada clase se ubica en una cola por separado y se le asigna un porcentaje del ancho de banda fijo. La salida de las colas es entonces liberada en un periodo de tiempo según su porcentaje asignado (figura 1.24).

CBQ es un método simple en el cual se da a todas las clases de servicio un rendimiento predecible y puede ser implementado en *hardware*.

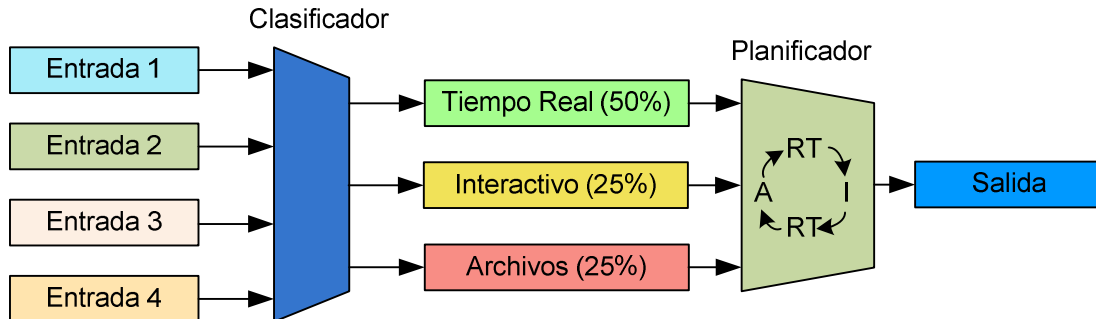


Figura 1.24 Diagrama de flujo de colas CBQ

1.3.6.4 Ingeniería de Tráfico con MPLS ^[19]

Con IP y el mecanismo de enrutamiento del camino más corto o por el menor número de saltos, a menudo se crean puntos de congestión, con alta probabilidad de descarte de paquetes, mientras otras rutas posibles están poco cargadas. Éste es un problema de optimización de rendimiento de la red y es difícil de relacionar con una baja calidad de servicio. MPLS posee un mecanismo de *enrutamiento explícito* que permite especificar, de salto a salto, el camino de los circuitos virtuales que crea. De esta manera se pueden utilizar los recursos de la red que estén desocupados, aumentando el rendimiento global de la red.

El proceso de optimizar el rendimiento de las redes a través del eficiente aprovisionamiento de recursos y el mejor control de los flujos en la red, es referido comúnmente como Ingeniería de Tráfico, presente en MPLS.

Además de la Ingeniería de Tráfico, la adición de conceptos de IntServ y DiffServ, como la reserva de ancho de banda sobre un LSP (*Label Switched Path*) o la etiquetación de los paquetes para indicar su prioridad, hacen de MPLS una excelente opción para que, junto a IP, formen una infraestructura eficiente de entrega de paquetes con calidad de servicio.

1.3.7 COMUNICACIONES UNIFICADAS ^{[25][26][27][50][53]}

En el mundo tecnológico de las comunicaciones actuales es común encontrarse con términos como Telefonía IP, convergencia, mensajería unificada, presencia, etc. La idea detrás de todos estos términos es la posibilidad de que las personas estén en contacto unas con otras sin importar dónde se encuentren, y según sus necesidades puedan comunicarse a través del medio más apropiado.

En sus inicios, la Telefonía IP cumplía los requerimientos de comunicaciones dentro de una organización, sin explotar de manera adecuada sus capacidades. Las organizaciones que adoptaban la Telefonía IP seguían siendo poco eficientes y productivas, sus usuarios necesitaban un sistema de comunicaciones variado y flexible que satisfaga las necesidades de su negocio.

El desarrollo de nuevas aplicaciones acordes a las necesidades de la organización permitió la integración de servicios de datos, voz y video en una infraestructura convergente. La unión de dispositivos y servicios de datos, voz y video permitían a los usuarios comunicarse de manera rápida y eficiente, con la facilidad de utilizar varias aplicaciones a través de una sola infraestructura; fue así como nació el concepto de comunicaciones unificadas (UC, *Unified Communications*).

Comunicaciones Unificadas es la tecnología que referencia a toda clase de comunicaciones y las características de administración de estos medios, controlados ya sea por un único usuario o de otra manera por funciones personales o de negocios. Comunicaciones Unificadas abarca generalmente a casi todos los avances tecnológicos encontrados hoy: correo de voz, correo electrónico, Voz sobre IP, *streaming* de audio y video, web y teleconferencia, sistemas de mensajería unificada, correo de voz unificado, etc. UC integra los sistemas de comunicación fijos y móviles, en un estilo de comunicación siempre disponible.

Existen dos elementos que le dan la forma que hoy se conoce de UC: Mensajería Unificada y Colaboración en Tiempo Real.

1.3.7.1 Mensajería Unificada ^[26]

Mensajería Unificada es el término usado para denotar la fusión o el proceso de combinar tecnologías como: correo de voz, FAX, correo electrónico, SMS, MMS (mensajería de texto), etc. en un repositorio de almacenamiento unificado, conocido como el buzón de mensajes.

El buzón de mensajes es capaz de ser accedido desde casi cualquier dispositivo de comunicaciones personales como el computador o el teléfono. El acceso se lo realiza por medio de clientes de correo vía web o *software* específico como *MS Outlook*. En vista de que los dispositivos de acceso tienen capacidades multimedia, el buzón puede contener voz, video o datos. Además, el contenido tipo FAX puede ser guardado o impreso según se necesite. Sin embargo, Mensajería Unificada es sólo un subconjunto de las Comunicaciones Unificadas.

1.3.7.2 Colaboración en Tiempo Real ^[28]

El objetivo de la colaboración entre varios individuos es obtener mejores resultados que los que puede conseguir uno solo de ellos. Las herramientas de colaboración en tiempo real precisamente están diseñadas para cumplir ese objetivo. La mensajería instantánea, las conferencias de audio o video y las pizarras virtuales permiten a los participantes intercambiar ideas e información de forma rápida e interactiva en cualquier parte del mundo; esto hace la colaboración lo más natural posible, semejándose cada vez más a reuniones cara a cara.

Los servicios en tiempo real son preferidos por mejorar los tiempos de respuesta y la resolución de problemas al momento en el que se presentan.

La Mensajería Unificada y la Colaboración en Tiempo Real son las soluciones que hoy se presentan como Comunicaciones Unificadas. Cada una de ellas permite al

usuario entregar y recibir la información de la manera, el momento y al público pertinentes. UM, tiene como característica el almacenamiento de los mensajes que no necesitan o no pueden ser entregados directamente al destinatario el momento del envío. Por el contrario, RTC se distingue por contar con la presencia de los participantes durante la reunión o *meeting* virtual. Saber dónde entregar un mensaje a un individuo o cómo contactarlo para un *meeting* marca la necesidad de determinar su ubicación.

1.3.7.3 Presencia ^{[29][51]}

El hogar, la oficina, la carretera, un aeropuerto, etc. son lugares donde probablemente puede encontrarse un individuo el momento de ser contactado. Teléfonos celulares, computadores de escritorio, computadores portátiles, GPS, entre otros, son dispositivos que un usuario puede usar para acceder a una red. En vista de que el número de dispositivos y lugares desde los cuales el usuario puede acceder a una red es muy amplio, es imposible asociarlo con uno sólo de ellos en determinado momento.

Presencia es el concepto de comunicaciones unificadas para definir cuándo, dónde y qué se encuentra haciendo un usuario; es decir, la disponibilidad de un individuo en un instante dado. Presencia es una parte fundamental de comunicaciones unificadas, sobre todo a tiempo real, ya que agiliza el proceso de contactar a los usuarios al tener en cuenta su localización y estado de actividad.

1.3.7.4 Servicios en Comunicaciones Unificadas ^{[25][26][28][29][51][53]}

Las comunicaciones unificadas, en una organización, tienen como objetivo incrementar la productividad. La flexibilidad en las comunicaciones permite optimizar los procesos de trabajo y ahorrar tiempo para cumplir las metas de la organización.

Los servicios más comunes que se integran dentro de las comunicaciones unificadas son:

- **Telefonía.** Las comunicaciones de voz con los clientes de la organización y entre empleados refuerzan sus relaciones e incrementan la productividad. Los empleados necesitan realizar llamadas a los clientes de forma fácil y rápida, razón por la cual se integró el teléfono con el computador. Además, la aparición de nuevas tecnologías de redes de datos como VoIP permitió la integración de las redes de voz y datos facilitando el desarrollo de nuevas funcionalidades a las ya conocidas por la Telefonía tradicional.
- **Mensajería Asincrónica.** Es un servicio que permite a los usuarios el envío y recepción de mensajes, donde el tiempo de envío es irrelevante. En este servicio es importante la integridad del mensaje transmitido. Incluye el envío y recepción de mensajes de texto, fax, correo electrónico, SMS, MMS, etc. Además, admite que se adjunten archivos a los mensajes de texto; sean éstos de audio, video o documentos.
- **Mensajería Instantánea.** Es un servicio de red que permite a los usuarios el envío y recepción de mensajes de texto en tiempo real. El usuario necesita tener un cliente de mensajería instantánea y estar conectado a una red de datos como el Internet. Existen dos tipos de clientes: los *remitentes* y las *bandejas de entrada instantáneas*, donde se reciben los mensajes. Un remitente proporciona mensajes instantáneos al servicio de mensajería instantánea. Estos mensajes son enviados en base a una dirección a su correspondiente bandeja de entrada instantánea. Los mensajes instantáneos trabajan conjuntamente con los servicios de presencia.
- **Presencia.** Es un servicio que permite proveer información del estado de una persona en un determinado instante de tiempo para establecer su localización. Este servicio es uno de los principales dentro de las funciones de UC ya que con él se realizan la mayor parte de aplicaciones que se pueden encontrar en el mercado y que benefician a las organizaciones. Dentro de presencia se distinguen los siguientes tipos: *presencia básica*, el usuario puede decir de manera indirecta a otro que está disponible para que lo contacten, evitando así la pérdida de tiempo al realizar una llamada sin que ésta tenga éxito. *Presencia enriquecida*, informa sobre la interacción que tiene el usuario con sus dispositivos. *Presencia contextual*,

permite al usuario expresar la actividad que está realizando en ese momento o dónde se encuentra en el caso de ausentarse de su ubicación habitual; es decir, es un servicio inteligente para que el sistema pueda determinar el estado de una persona. *Presencia de progreso*, indica la disponibilidad de un usuario, a través de una estimación de tiempo al final de la cual se espera que el usuario haya terminado una actividad específica.

- **Conferencia.** Servicio donde varios participantes, usualmente tres o más, intercambian información en tiempo real. Otros participantes pueden adherirse o salir de la conferencia luego que ésta ha iniciado. Se hace uso de capacidades multimedia como audio, video, texto, datos u otras herramientas. Durante una conferencia es factible la activación de una u otra capacidad multimedia de acuerdo a la conveniencia, y no es necesario que los dispositivos de todos los participantes compartan las mismas funcionalidades.

La combinación de dos o más servicios provistos por las comunicaciones unificadas permite el desarrollo de aplicaciones de acuerdo a los requerimientos de una organización. El desarrollo de estas aplicaciones dependerá de cada fabricante, es por ello que cada fabricante oferta sus equipos con aplicaciones por defecto.

1.3.7.5 Aplicaciones con Comunicaciones Unificadas ^{[54][53][57]} – [64]

En la mayoría de organizaciones los empleados son móviles, es decir, por algún motivo laboral deben trasladarse de sus puestos de trabajo y muchos de ellos fuera de la organización. Esta movilización genera un gran problema en las comunicaciones. Existen muchos dispositivos que los empleados utilizan para comunicarse, pero al no estar integrados es difícil tener la certeza de concretar una comunicación. Al inicio, esta dificultad puede ser vista simplemente como incómoda pero posee consecuencias económicas reales. Las aplicaciones de comunicaciones unificadas pueden brindar una ventaja competitiva y cierta inteligencia en las comunicaciones entre empleados. Para ello es necesario

dimensionar las aplicaciones que necesita una organización. En la figura 1.25 se puede observar las ventajas que se encuentran en una infraestructura de comunicaciones IP.

Se pueden desarrollar más aplicaciones donde se integren varios servicios de comunicaciones unificadas, entre las cuales se pueden encontrar:



Figura 1.25 Ventajas de una infraestructura de comunicaciones IP

- **Telepresencia.** Es una aplicación derivada de la conferencia donde se tiene la sensación de estar físicamente en otro sitio, mediante equipos multimedia. Para la telepresencia se debe disponer de una pantalla panorámica y altavoces de sonido envolvente y cámaras de alta definición (figura 1.26). Su implementación proporciona importantes beneficios, como el trabajo colaborativo entre personas geográficamente distantes y una mayor integración entre grupos de trabajo.
- **Pizarra virtual.** Esta aplicación permite a varios usuarios tener una vista común sobre un documento o imagen y poder interactuar en un proceso de colaboración realizando cambios para obtener resultados grupales.
- **Asistente virtual.** Los asistentes virtuales son aplicaciones computarizadas que gestionan actividades administrativas de un usuario; se suelen integrar a la mensajería unificada permitiendo de esta manera

acceder desde cualquier dispositivo o servicio, para conocer las actividades administrativas.

- **Compartición de archivos en tiempo real.** Mientras se mantiene una conversación telefónica se puede enviar archivos y ser vistos en tiempo real, facilitando la colaboración y resolución de problemas.
- **Conversión Texto/Voz.** Con la unificación de la mensajería de voz y texto en un solo buzón, y el avance de los algoritmos y procesadores digitales de la voz se hizo viable convertir la voz en texto y viceversa. Esta función, conocida como Reconocimiento de Voz y *Text-to-Speech* se oferta en productos de mensajería unificada principalmente.



Figura 1.26 *Telepresencia*

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 1

LIBROS

- [1] TANENBAUM Andrew, “Computer Networks”, Cuarta Edición, Edit. Prentice Hall, Marzo 2003, Págs. 37 – 46
- [2] HIDALGO Pablo, “Folleto de Redes de Área Local”, EPN, 2008
- [3] SEIFERT Rich, “The Complete Guide to LAN Switching Technology”, Segunda Edición, Edit. John Wiley & Sons, 2008, Págs. 5 – 9
- [4] SOSINSKY Barrie, “Networking Bible”, Edit. Wiley Publishing, Canadá 2009
- [5] GONZÁLEZ Fabio, “Diapositivas de Sistemas de Cableado Estructurado”, 2008
- [6] BARNETT David, “Cabling: The Complete Guide to Networking Wiring”, Tercera Edición, Edit. Sybex, 2004, Págs. 4 – 8
- [7] HIDALGO Pablo, “Folleto de Redes de Área Extendida”, EPN, 2009
- [8] JAVVIN TECHNOLOGIES, “Network Protocols Handbook”, Segunda Edición, 2005
- [9] BELLAMY John, “Digital Telephony”, Tercera Edición, Edit. John Wiley & Sons, Canadá 2000
- [10] BIGELOW Stephen, “Understanding Telephone Electronics”, Cuarta Edición, Edit. Newnes – Butterworth-Heinemann, 2001
- [11] GREEN James Harry, “The Irwin Handbook of Telecommunications”, Quinta Edición, Edit. McGraw-Hill, USA 2006, Págs. 195 – 206
- [12] BROWN Kevin, “IP Telephony Unveiled”, Edit. CISCO Press, Enero 2004
- [13] WALLINGFORD Theodore, “Switching to VoIP”, Edit. O’Reilly, Junio 2005
- [14] KUMAR Vineet, “IP Telephony with H.323. Architectures for Unified Networks and Integrated Services”, Edit. John Wiley & Sons, Canadá 2001
- [15] JOHNSTONE Alan B., “SIP. Understanding the Session Initiation Protocol”, Segunda Edición, Edit. Artech House, 2004
- [16] RUSSELL Travis, “Session Initiation Protocol, (SIP). Controlling Convergent Networks”, Edit. McGraw-Hill, 2008, Págs. 46 – 48
- [17] CHAFFIN Larry, “Building a VoIP Network with Multimedia Communication Server 5100”, Edit. Syngress, 2006, Págs. 346 – 376

- [18] RFC 3261, "SIP: Session Initiation Protocol", ROSENBERG, J., Junio 2002
<http://datatracker.ietf.org/doc/rfc3261/>
- [19] FARREL Adrian, "Network Quality of Service. Know it all", Edit. Morgan Kaufmann – Elsevier, 2009, Págs. 1 – 11,
- [20] ELLIS Juanita, "Voice, Video and Data Convergence: Architecture and Design, from VoIP to Wireless", Edit. Academic Press, USA 2003, Págs. 90 – 97
- [21] SZIGETI Tim, "End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs", Edit. CISCO Press, Noviembre 2004
- [22] PUJOLLE Guy, "Management, Control and Evolution of IP Networks", Edit. ISTE, Gran Bretaña 2007
- [23] MASAM Peter, "Managing Service Level Management Across Wireless and Fixed Networks", Edit. John Wiley & Sons, 2003, Págs. 97 – 102
- [24] GREGORY Peter H., "Comunicaciones Unificadas para Dummies", Edit. Wiley Publishing, 2008
- [25] CARTER Jeff, "Unified Communications 100 Success Secrets. Discover the Best Way to Unify Your Enterprise, Covers Unified Messaging, Systems, Solutions, Software and Services", 2008, Págs.
- [26] STAIR Ralph, "Principles of Information Systems", Novena Edición, Edit. Course Technology, Enero 2009
- [27] COLEMAN David, "Collaboration 2.0. Technology and Best Practices for Successful Collaboration in a WEB 2.0 World", 2008, Págs. 26 – 27
- [28] RFC 2778, "A Model for Presence and Instant Messaging", DAY, M.
<http://datatracker.ietf.org/doc/rfc2778/>
- [29] CALERO Alejandro. "Redes telefónicas públicas conmutadas: Oportunidades de desarrollo profesional". PDF; 1998
- [30] CARRASCO José Manuel. "EVOLUCIÓN HISTÓRICA DE LA CONMUTACIÓN TELEFÓNICA", pdf; 2001.

PROYECTOS DE TITULACIÓN

- [31] Domínguez Andrés, "Análisis de Implementación y Recomendación de Soluciones Corporativas de Comunicaciones Unificadas *NGN Based* con

Business Communications Manager (BCM) de NORTEL”, Quito, Junio 2009

INTERNET

- [32] CISCO. CCNA_Exploration_v4. "Conmutación y conexión inalámbrica de LAN". Cap 3.
- [33] WIKIPEDIA. "VLAN"
<http://es.wikipedia.org/wiki/VLAN>
- [34] TEXTOS CIENTÍFICOS. "Redes Virtuales VLANs"
<http://www.textoscientificos.com/redes/redes-virtuales>
- [35] ANÓNIMO. "VLAN"
http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf
- [36] KIOSKEA. "MPLS - Conmutación de etiquetas multiprotocolo"
<http://es.kioskea.net/contents/internet/mps.php3>
- [37] CANALIS, Sol María. "MPLS "Multiprotocol Label Switching": Una Arquitectura de Backbone para la Internet del Siglo XXI"
<http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MPLS.PDF>
- [38] KIOSKEA. "Equipos de red - El concentrador"
<http://es.kioskea.net/contents/lan/concentrateurs.php3>
- [39] ANÓNIMO, "Telefonía IP en el Entorno Corporativo (primera parte)"
http://aleros.blogspot.com/2005_10_01_aleros_archive.html
- [40] Grupo de Expertos sobre Telefonía IP del UIT-D, "Informe Esencial sobre Telefonía IP", UIT 2003
http://www.itu.int/ITU-D/cyb/publications/2003/IP-tel_report-es.pdf
- [41] ÁVILA Nelson, Presentación "Principios de Telefonía IP", 2009 mayo.
- [42] VOIPFORO. "Objetivo H.323"
<http://www.voipforo.com/H323/H323objetivo.php>
- [43] KIOSKEA. "RTP/RTCP protocols"
<http://en.kioskea.net/contents/internet/rtcp.php3>
- [44] ANONIMO. "Real-time Transport Protocol"

- http://es.wikipedia.org/wiki/Real-time_Transport_Protocol
- [45] ANONIMO. "Real time control protocol"
<http://es.wikipedia.org/wiki/RTCP>
- [46] UBIQUITY, "Understanding SIP. Today's Hottest Communications Protocol Comes of Age"
http://www.brissongroup.com/pdf/whitepapers/UnderstandSIP_WP.pdf
- [47] DOUMAS Thomas, "Next Generation Telephony: A Look to Session Initiation Protocol", AGILENT Technologies
<http://www.pulsewan.com/data101/sip.pdf>
- [48] IREK Florin, "The Architecture of an Integrated RTSP, RTP and SDP Library"
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.9084&rep=rep1&type=pdf>
- [49] ANÓNIMO, "Calidad de Servicio"
<http://www.slideboom.com/presentations/100915/calidad-de-servicio>
- [50] PRAHL Alfredo, "COMUNICACION UNIFICADA, QUE ES Y PORQUE DEBE IMPORTARLE?", 2007
http://blogs.technet.com/alfredo/archive/2007/07/24/Comunicacion-unificada-que-es-y-porque-debe-importarle_2E00_.aspx
- [51] URDIALES Diego. "Servicios de presencia enriquecida instantánea – Más allá de la Twitter-revolución"
<http://www.lacofa.es/index.php/innovacion/servicios-de-presencia-enriquecida-instantanea-mas-alla-de-la-twitter-revolucion>
- [52] THOMPSON Paul. "Comunicaciones unificadas". Panasonic. Abril 2008
http://www.revistaitnow.com/pdfs/PDF_Tech_Day/Comunicaciones_Unificadas_PANASONIC.pdf?phpMy
- [53] SHORETEL. "Estableciendo Las Bases Adecuadas: Comunicaciones Unificadas"
www.shoretel.eu/es/downloads/unified_communications_whitepaper_es.pdf
- [54] CISCO. "Aplicaciones de Comunicaciones Unificadas: Usos y ventajas"
http://www.cisco.com/web/LA/soluciones/comercial/Aplicaciones_de_Comunicaciones_Unificadas_Sage_Esp_2006.pdf
- [55] INNOVATECNO. "Sistemas de Telepresencia"

<http://www.innovatecno.com/TelepresenciaRV.php>

[56] CARRIÓN Hugo "Apuntes de Sistemas de Telefonía", 2007

VIDEOS

[57] NORTEL. "Telepresencia publicidad"

<http://www.youtube.com/watch?v=Mxy44rckeBA>

[58] CISCO. "Relepresence"

<http://www.youtube.com/watch?v=gOjfmRVz1OM&feature=related>

[59] CISCO. "Cisco Unified Communications"

<http://www.youtube.com/watch?v=h8Lq9X0Qv94>

[60] AVAYA. "Comunicaiones unificadas de Avaya en arquitectura"

http://www.youtube.com/watch?v=HkCeosIKR_M

[61] AVAYA. "Comunicaciones unificadas de avaya en tu industria"

<http://www.youtube.com/watch?v=jkuKwaZGjYI&feature=related>

[62] MICROSOFT. "El diablo viste a la moda"

<http://www.youtube.com/watch?v=SKrSb9Ac-UQ>

FOTOS

[63] ANÓNIMO. "Telepresencia"

<http://elultimoquecierrelapuerta.files.wordpress.com/2007/12/telepresencia.jpg>

[64] ANONIMO. "Imagen Telepresencia"

http://www.infolatam.com/img/banco/5629G_LATERAL_GRUPO.jpg

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL Y REQUERIMIENTOS

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En el presente capítulo se establecerá el estado en el que se encuentra la empresa Alianza de Seguros, junto con su red de datos y Telefonía. Con esta información y los lineamientos tecnológicos de la empresa, se determinarán los requerimientos para el diseño de la nueva red, que incluirá Telefonía IP.

A continuación se presentan las características administrativas de la compañía.

2.1.1 ALIANZA COMPAÑÍA DE SEGUROS Y REASEGUROS S.A. ^[4]

Alianza Compañía de Seguros y Reaseguros S.A. es una entidad financiera ecuatoriana, dedicada al negocio de los seguros generales desde hace más de 28 años. Su trabajo es brindar seguridad a sus clientes por medio de la compartición de riesgos ante posibles eventualidades, así como minimizar su propio riesgo al contratar los servicios de reaseguradoras locales e internacionales.

2.1.1.1 Misión ^[4]

“Cumplir las obligaciones con nuestros clientes y accionistas, con capital humano comprometido en el desarrollo de productos innovadores, empleando tecnología de punta.”

2.1.1.2 Visión ^[4]

“Ser la compañía de seguros generales líder en el mercado ecuatoriano, con productos innovadores superando con excelencia las necesidades de nuestros clientes internos y externos generando la más alta rentabilidad.”

2.1.1.3 Situación Actual de Alianza de Seguros

Alianza cuenta con oficinas en algunas de las principales ciudades del Ecuador: Quito, Guayaquil, Cuenca, Manta, Santo Domingo de los Colorados, Machala y Milagro. Las ciudades más importantes para la empresa, donde se concentra el mayor número de empleados y la gerencia, son Quito y Guayaquil; las demás sucursales son dependientes de las oficinas de Quito.

2.1.1.3.1 Distribución de las Instalaciones en Quito y Guayaquil

La matriz de Alianza se encuentra ubicada en Quito en la Av. 12 de Octubre N 24-359 y Baquerizo Moreno y cuenta con tres áreas: el edificio principal, una planta independiente y un parqueadero. La localización geográfica se muestra en la figura 2.1



Figura 2.1 Instalaciones de Alianza en Quito

El edificio principal, peculiar por su estructura arquitectónica en forma de castillo (ver figura 2.2), contiene cuatro plantas: subsuelo, planta baja, primer piso y segundo piso. Cada una de las plantas alberga a distintos ambientes o áreas de trabajo según los departamentos de Alianza en Quito. La distribución de los ambientes y áreas de trabajo se especifica en la tabla 2.1 y se puede observar en los planos del anexo A.



Figura 2.2 Castillo Larrea. Oficinas de Alianza en Quito

Planta		Ambiente/Departamento
Edificio Principal	SB	Archivo Caja Cobranzas Emisión Reaseguros Siniestros Siniestros-SOAT
	PB	Brokers Gerencias Producción Recepción
	P1	Contabilidad RRHH Sala de Reuniones Sistemas
	P2	Comedor Terraza
Planta Independiente		Extern Solut Suite Guardianía

Tabla 2.1 Distribución de ambientes y departamentos en Quito

En Guayaquil existen dos oficinas. La principal se encuentra ubicada en el centro de la ciudad, en la intersección de las Av. 9 de Octubre y G. Córdova, edificio San Francisco 300, onceavo piso. La segunda oficina, ubicada en el sector de la

Kennedy al norte de la ciudad, se considera una sucursal más, dependiente de Quito.

Las oficinas de Alianza en el centro de Guayaquil ocupan todo el onceavo piso del edificio San Francisco 300, el cual se encuentra dividido en dos alas. Las alas, separadas por el pasillo de ingreso, contienen los ambientes y departamentos enumerados en la tabla 2.2.

Ala	Ambiente/ Departamento
1	Gerencias Sala Reuniones Producción Recepción SOAT
2	Sistemas Cobranzas Emisión Siniestros Caja Brokers Comedor

Tabla 2.2 *Distribución de ambientes y departamentos en Guayaquil – Centro*

2.1.1.3.2 Estructura organizacional de Alianza de Seguros

La empresa está formada por departamentos, según la estructura organizacional que se muestra en la figura 2.3. A la cabeza de la organización se encuentra la Junta de Accionistas, seguida del Directorio General. La presidencia ejecutiva toma las decisiones cruciales para Alianza y la Gerencia General tiene a su cargo la coordinación de las gerencias: Financiera, Técnica, Comercial, Reaseguros y de sucursales. El área de operaciones y el área comercial son las que reflejan el negocio de la compañía. En ellas se realizan los trámites de emisión de pólizas de seguros, recepción de reclamos, renovaciones de pólizas, etc. La responsabilidad de la administración financiera es tener al día pagos, primas de seguros y todos los rubros económicos de la empresa.

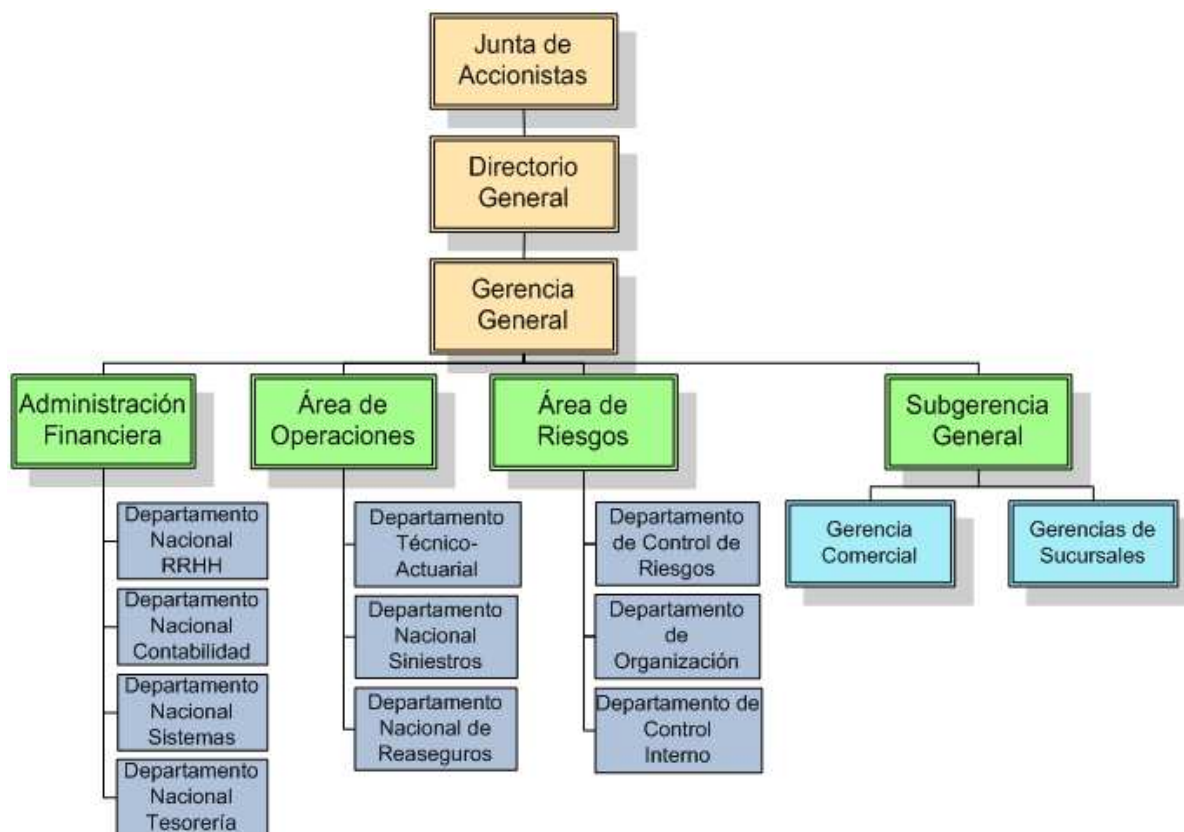


Figura 2.3 Estructura organizacional de Alianza de Seguros

2.1.1.3.3 Características del Personal de Alianza

El personal de Alianza está repartido entre las diferentes sucursales alrededor del Ecuador. El número de empleados varía de acuerdo a las necesidades de la empresa. A medida que el negocio de los seguros evoluciona, los departamentos en Alianza se incrementan, se fusionan, se remueven, se aumentan sucursales, etc., lo que ocasiona que el personal varíe. En la actualidad, Alianza cuenta con cerca de 137 empleados a nivel nacional que, en su mayoría, se concentran en las ciudades de Quito y Guayaquil, según se puede apreciar en la tabla 2.3.

De forma regular, el personal administrativo, de operaciones y de mantenimiento realiza sus labores al interior de las instalaciones de la empresa. Son algunos miembros del personal los que, por razones laborales, deben realizar sus funciones desde fuera de las instalaciones o con traslados constantes; de los

cuales se puede citar al Presidente Ejecutivo, al *Gerente General*, personal de cobranzas e inspectores de siniestros.

Sucursal	Número Empleados
Quito (Matriz)	57
Guayaquil Centro	32
Cuenca	20
Manta	11
Santo Domingo	8
Milagro	6
Guayaquil Kennedy	6
Machala	4
Total	137

Tabla 2.3 *Número de empleados de Alianza*

La presidencia se ejerce desde España, donde reside el Presidente Ejecutivo. Las gerencias de la empresa están distribuidas entre la matriz de Quito y las oficinas del centro de Guayaquil. Aunque la *Gerencia General* se encuentre oficialmente en la matriz de Quito, se dispone de otra oficina en Guayaquil para este mismo fin, debido a que el *Gerente General* pasa la mayor parte de su tiempo en esta ciudad.

Las actividades que se llevan a cabo al interior de Alianza consisten en la atención al cliente y a *brokers* (agentes de seguros), recepción de vehículos accidentados o por motivo del SOAT, cancelaciones de pólizas, etc., actividades que se encuentran soportadas en su mayoría por un sistema informático, el cual les permite acceder a toda la información necesaria desde el escritorio con un computador. Desde esta perspectiva, las necesidades de movilidad dentro de la empresa son mínimas, por lo que el personal de Alianza puede considerarse fijo en relación a su puesto de trabajo. En las tablas 2.4 y 2.5 se muestra la distribución del personal dentro de las instalaciones de Alianza en Quito y Guayaquil.

Piso (Empleados)	Departamento	Empleados
SB (24)	Siniestros	6
	Caja	2
	Cobranzas	5
	Siniestros-SOAT	3
	Emisión	4
	Archivo	2
	Reaseguros	2
PB (11)	Producción	4
	Gerencia	6
	Recepción	1
P1 (11)	Contabilidad	4
	RRHH	4
	Sistemas	3
	Sala de Reuniones	0
	Brokers	0
P2 (2)	Capilla	0
	Comedor	2
PI* (9)	Extern-Solut	7
	<i>Suite</i>	1
	Guardianía	1
TOTAL		57

* PI: Planta Independiente

Tabla 2.4 *Distribución del personal en Alianza Quito*

ALA (Empleados)	Departamento/Ambiente	Empleados
ALA1 (12)	Producción	4
	Recepción	1
	SOAT	2
	Sala de Reuniones	0
	Gerencia Técnica	1
	<i>Gerencia General</i>	1
	Gerencia Nacional	1
	Asistente Gerencia	2
ALA2 (20)	Sistemas	1
	Cobranzas	6
	Emisión	3
	Siniestros	4
	Caja	4
	Comedor	1
	Guardianía	1
TOTAL		32

Tabla 2.5 *Distribución del personal en Alianza Guayaquil*

Debido a la importancia de las oficinas de Quito y Guayaquil, a que cubren más del 60% del personal y a las facilidades que se han tenido para recabar información y constatar la situación actual de la empresa se procederá con la reingeniería de la red para estas dos oficinas.

2.1.2 ANÁLISIS DE LA RED DE DATOS

Alianza de Seguros cuenta con una red corporativa compuesta por las redes locales de cada una de sus sucursales y los enlaces WAN que las interconectan. El principal servicio que se brinda sobre esta red es el de base de datos que, en conjunto con otros servicios, son el soporte informático para las operaciones de la compañía.

2.1.2.1 Antecedentes

Desde sus inicios la empresa contaba con tecnología de punta para sus operaciones. Dentro de las instalaciones en la ciudad de Quito se disponía de un servidor IBM AS-36 que prestaba los servicios de compartición de archivos al personal de la empresa. Esto permitía la colaboración, el trabajo grupal y el ahorro de recursos humanos en los negocios. El personal accedía al servidor AS-36 conectándose con terminales no inteligentes a través de cable *thick-coaxial* con tecnología de red 10Base-2. Éste fue el primer paso dado en la evolución tecnológica.

Posteriormente, en el año 1992, debido al crecimiento de la empresa, se realiza la primera actualización del servidor AS-36 a la nueva versión de IBM, AS-400. Hasta ese año ya se identificaron las cualidades del servidor, lo cual representaba una importante ventaja competitiva, convirtiéndose en el núcleo que soporta todas las operaciones y transacciones del negocio hoy en día.

Para el año 2002, con el auge y crecimiento de las redes, se opta por las nuevas tecnologías de *networking*. De esta manera se introduce a la empresa: la tecnología *Fast Ethernet*, los enlaces de Internet; se cambian los terminales no

inteligentes por computadoras personales y se agregan algunos otros servicios, dejando al servidor AS-400 con la única funcionalidad de servidor de base de datos. A partir de esta fecha, se viene actualizando la infraestructura de la red aproximadamente cada dos años. Es así que la matriz en Quito se ha convertido en el centro tecnológico de las operaciones de la empresa, concentrando los principales equipos y servicios.

Actualmente, Seguros Alianza cuenta con una estructura de red centralizada, siendo Quito donde se encuentra concentrada la mayor parte de equipos que prestan servicios al personal y a los clientes de sus oficinas y sucursales. Las sucursales de las diferentes ciudades se conectan a Quito mediante enlaces dedicados, lo cual constituye la red WAN de Alianza. Cada sucursal cuenta con una red local que tiene algunos servicios propios, se enlaza a la red WAN y permite el acceso a los servicios centralizados de Quito.

2.1.2.2 Red LAN

Las redes LAN de Quito y Guayaquil son de tecnología *Fast Ethernet*, con una topología física en estrella. Se encuentran compuestas por elementos pasivos y activos: cableado estructurado, equipos de conectividad, servidores y dispositivos terminales.

2.1.2.2.1 Sistema de Cableado Estructurado

En las oficinas de Quito se tiene un sistema de cableado que viene funcionando desde hace siete años. Utiliza como medio de transmisión cable UTP categoría 5E con conectores RJ-45 para el cableado horizontal y vertical. Los puntos de red dentro del edificio se distribuyen según la tabla 2.6.

Las distintas áreas de trabajo distribuidas en el edificio se conectan a un solo cuarto de telecomunicaciones ubicado en el primer piso, en el Departamento de Sistemas, formando parte del cableado horizontal. El cableado horizontal se encuentra tendido sobre canaletas de plástico, aunque existen algunas áreas

donde se las ha retirado. En el Departamento de Sistemas se concentra el cableado y se lo enruta debajo del piso falso hacia el *rack* perteneciente al cuarto de telecomunicaciones.

QUITO				
Piso	# Puntos de red		# Impresoras Red	# PC's
	Ocupados	Libres		
SB	24	8	3	21
PB	12	1	1	12
P1	13	7	2	12
P2	0	0	0	0
*Extern	8	1	1	7
Total	57	17	7	52

* Extern Solut ocupa la planta independiente.

Tabla 2.6 Distribución de puntos de red en Alianza – Quito

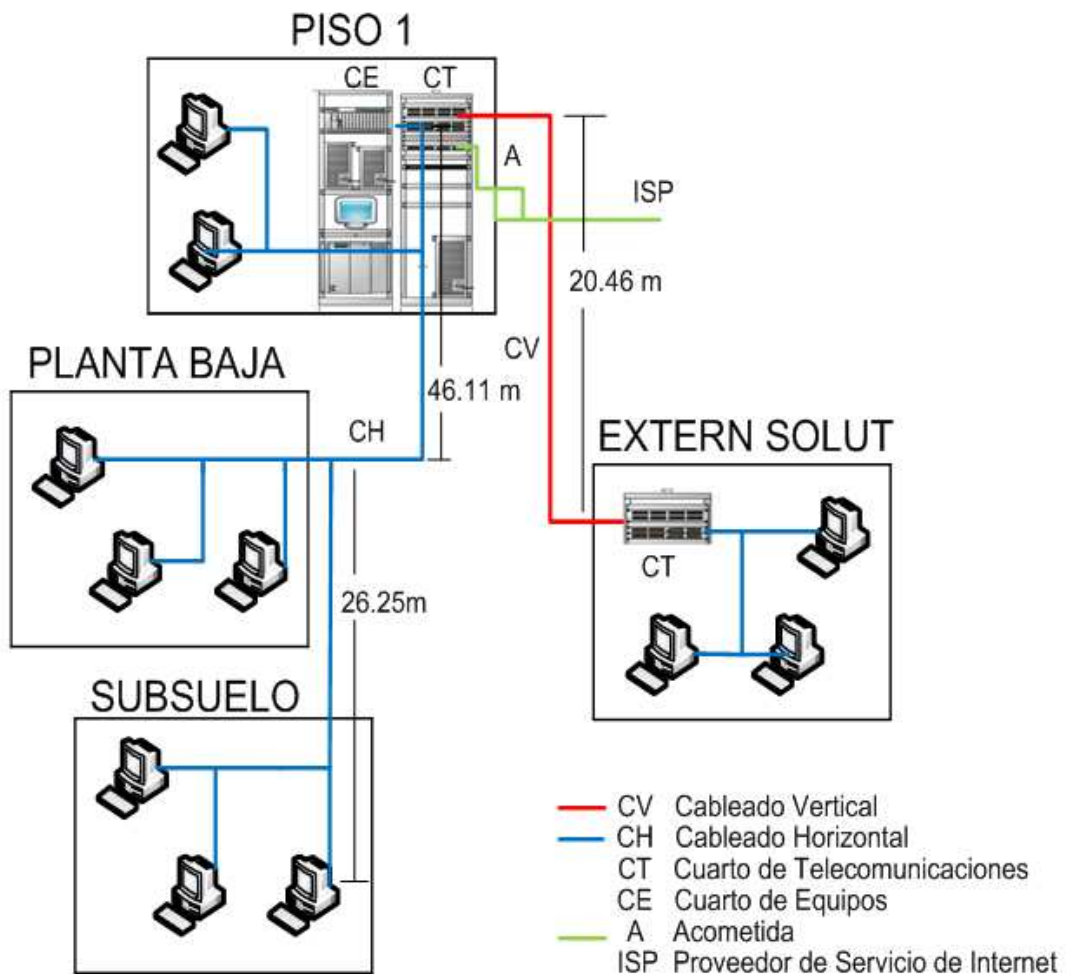


Figura 2.4 Distribución de cableado estructurado Quito

La interconexión entre el cuarto de telecomunicaciones del edificio principal con un *switch* de la planta independiente, perteneciente al Departamento Extern Solut, forma el cableado vertical. En la figura 2.4 se muestra la distribución del sistema de cableado estructurado.

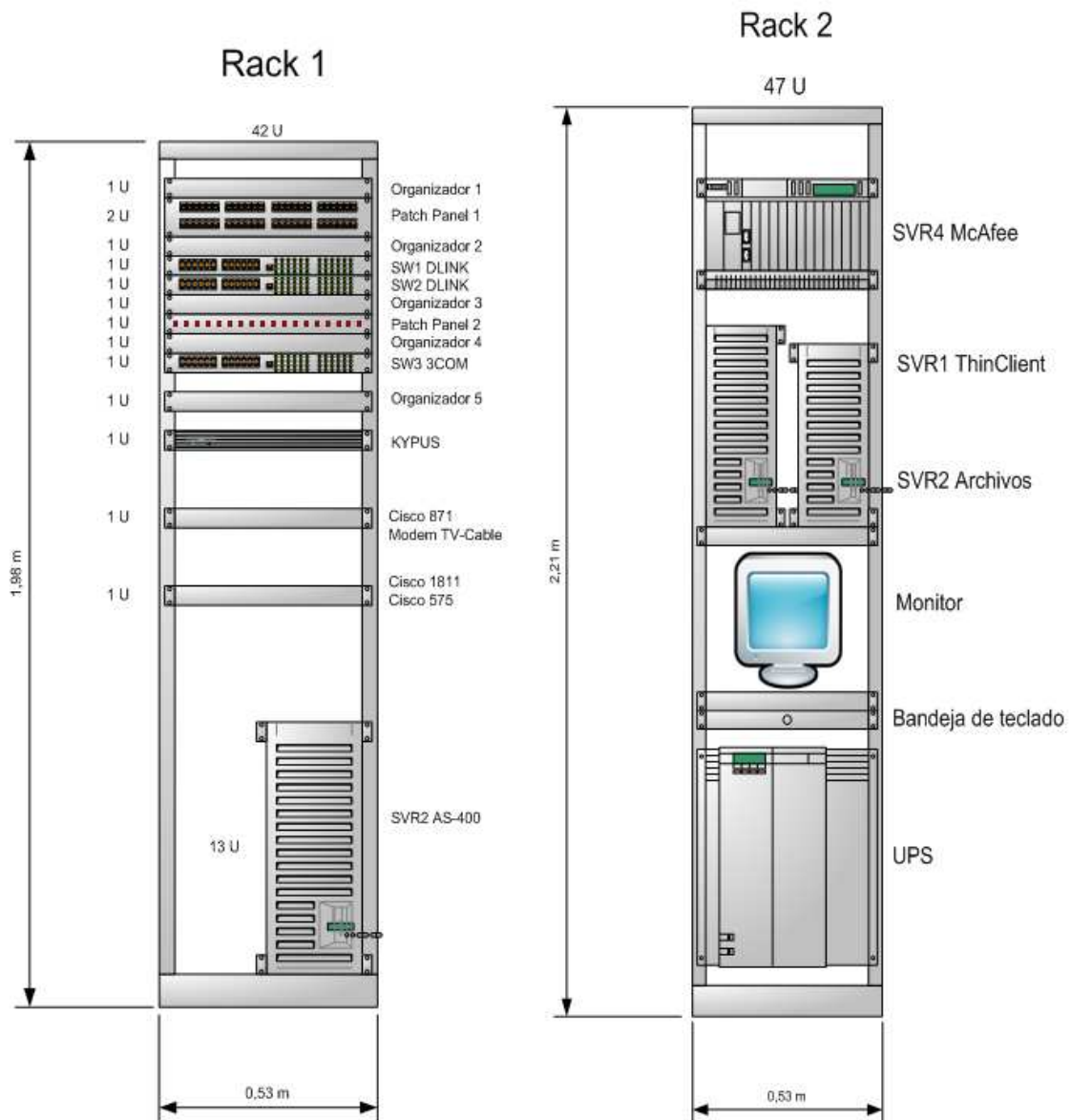


Figura 2.5 Distribución de equipos en los racks de Quito

El cuarto de equipos alberga todo los servidores de la empresa y se encuentra ubicado en el Departamento de Sistemas. Para el cuarto de equipos y de telecomunicaciones se cuenta con dos *racks* de 19", allí se ubican los equipos de conectividad y los servidores, como se muestra en la figura 2.5. Es importante

señalar la existencia de un servidor AS-400 adicional que no se encuentra dentro del rack por falta de espacio.

GUAYAQUIL							
Piso	# Puntos de red				# Impresoras Red	# Faxes	# PC's
	Ocupados		Libres				
	D	V	D	V			
Ala1	12	12	7	6	4	2	10
Ala2	18	19	4	3	4	2	15
Total	30	31	11	9	8	4	25

Tabla 2.7 Número de usuarios y número de equipos terminales

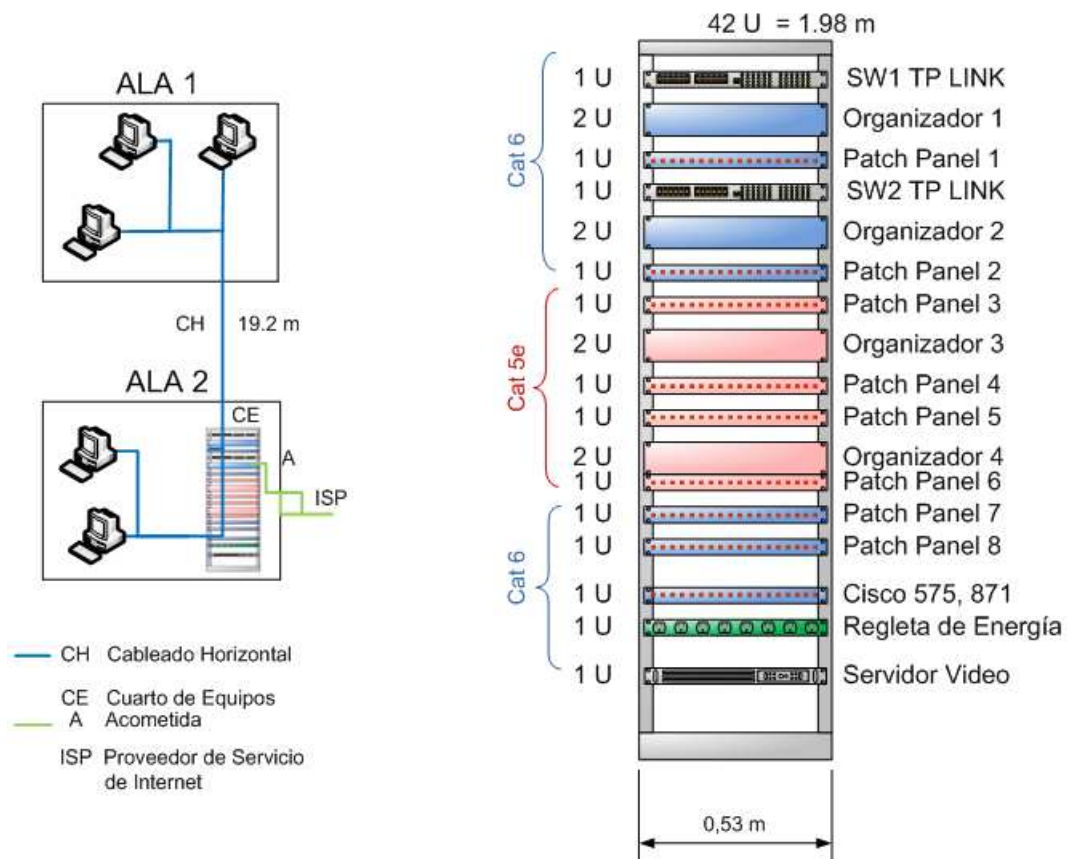


Figura 2.6 Distribución de cableado estructurado y equipos en rack de sucursal de Guayaquil

Para las oficinas de Guayaquil se cambió completamente el sistema de cableado estructurado, el cual está operando desde julio de 2009. El medio de transmisión utilizado es cable UTP categoría 6 para datos y cable UTP categoría 5e para voz,

con conectores RJ-45. En la tabla 2.7 se muestra la distribución de los puntos de red en las oficinas de Guayaquil.

El cableado horizontal se distribuye entre las dos alas del piso a través de ductos de PVC, para luego llegar a las estaciones de trabajo por medio de canaletas. Existe un solo cuarto de telecomunicaciones donde se concentra el cableado estructurado del Ala 1 y del Ala 2, ubicado en el Departamento de Sistemas. Éste cuenta con un *rack* de 19" donde se ubican los servidores, equipos de conectividad y elementos pasivos de la red (figura 2.6). No existe cableado vertical.

2.1.2.2.2 Equipos de Conectividad

Los equipos de conectividad que se encuentran instalados, tanto en las redes LAN Quito como Guayaquil, son de distintas marcas, en las que se encuentran: Cisco, 3COM, D-link, TP-Link, Encore, entre otras. La distribución de los equipos dentro de la red al igual que las funciones que cumplen, no siguen ningún modelo jerárquico de red o diseño establecido; su implementación obedece a las necesidades de la empresa y a su crecimiento. En las tablas 2.8 y 2.9 se detallan los equipos de conectividad actuales de la red con su respectiva ubicación.

QUITO				
SWITCHES				
Cantidad	Marca	Modelo	Ubicación	# Puertos
1	3Com	4200	Sistemas	24x10/100 2x10/100/1000
2	D-link	1024R ⁺	Sistemas	24x10/100
2	Encore	ENH905-NWY	RRHH Extern Solut	8x10/100
2	TrendNet	TE100- S5TE100-S5	Reaseguros Extern Solut	5x10/100
1	Linksys	SD208	Brokers	8x10/100
1	CNET	CSH-800	Sistemas	8x10/100
1	3Com	2016	Extern-Solut	16x10/100 2x10/100/1000

Tabla 2.8 Equipos de conectividad LAN Quito

GUAYAQUIL				
SWITCHES				
Cantidad	Marca	Modelo	Ubicación	# Puertos
2	TP-LINK	TL-SG1024	Sistemas	24-PORT GIGABIT ETHERNET SWITCH (10/1000)
3	D-LINK	DES-1008D	Sistemas	10/100 FAST ETHERNET SWITCH

Tabla 2.9 *Equipos de conectividad LAN Guayaquil*

La red LAN Quito tiene 10 *switches* que se interconectan entre sí y sirven para el acceso de estaciones de trabajo y servidores. Se tiene un único *switch* de marca 3COM que se conecta a un *router*, propiedad del *carrier*⁴, para permitir la interconexión entre las LAN de Quito, Guayaquil y las sucursales restantes. En la LAN Guayaquil se tiene únicamente 5 *switches* para la conexión de las estaciones de trabajo y servidores. En la figura 2.7 se muestra el esquema topológico de las LAN Quito y Guayaquil.

2.1.2.2.3 Servidores

Los usuarios de la red pueden emplear los siguientes servicios: base de datos, antivirus, *Thin-Client*, correo electrónico, servidor de archivos, WEB, DNS y *firewall*, los mismos que se encuentran concentrados en seis servidores. En la tabla 2.10 se detallan las características de los servidores y los servicios que brindan.

Según lo observado en la tabla 2.10, se tiene un servidor de video ubicado en Guayaquil que permite la vigilancia de las oficinas. A él tienen acceso el *Gerente General* y el Departamento de Sistemas de Guayaquil. Además, se puede observar que el servidor AS-400 presenta dos tarjetas de red de similares capacidades pero de las cuales sólo una tarjeta de red se utiliza, mientras que la otra se preserva como respaldo. La función de cada servidor se detallará más adelante, según el servicio que prestan.

⁴ *CARRIER* se denomina así a la empresa de telecomunicaciones que brinda servicios de transporte de datos.

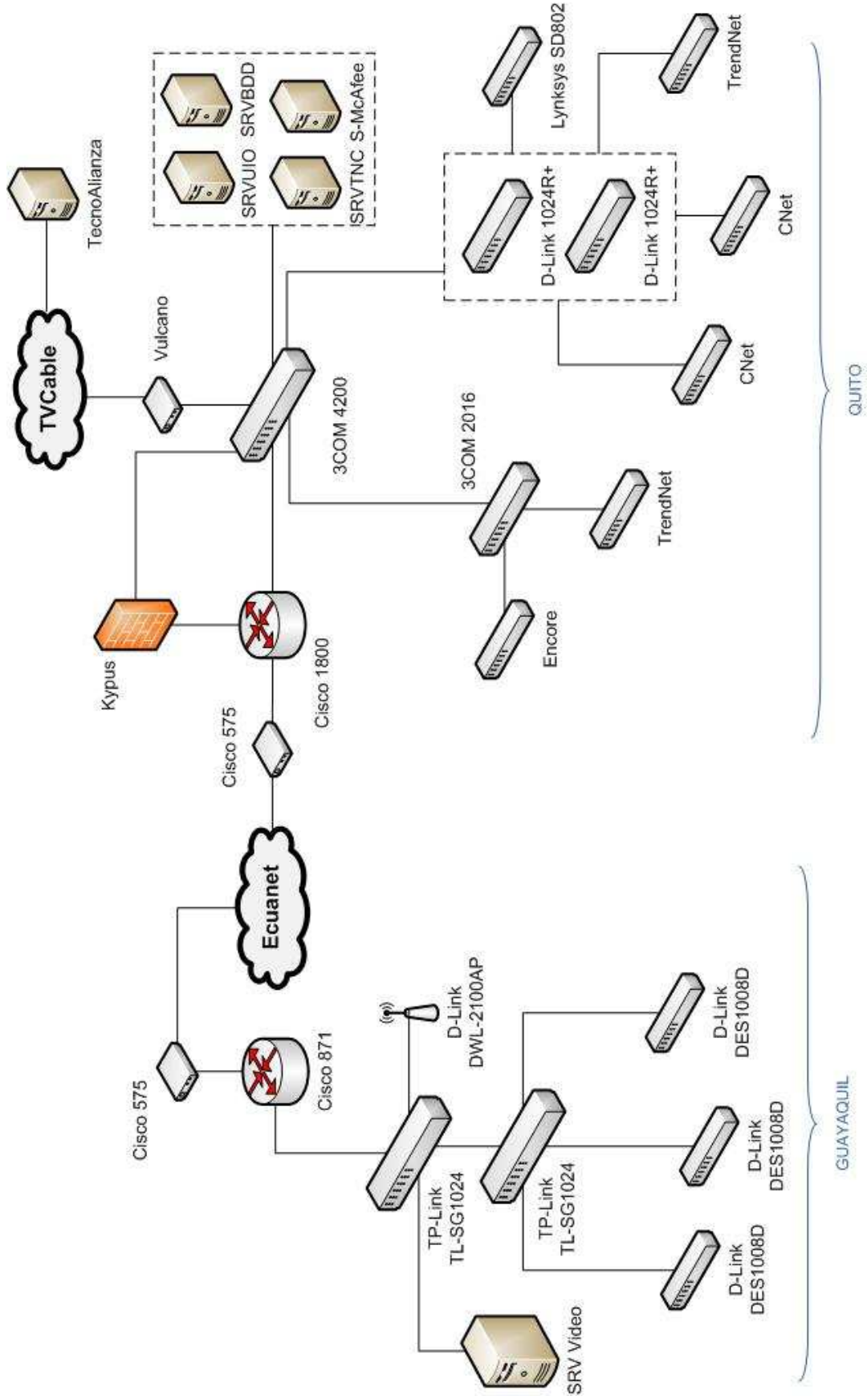


Figura 2.7 Esquema topológico de las LAN UJO y GYE

SERVIDORES EN QUITO											
Nombre	Marca	Procesador	Memoria [MB]			Disco Duro [GB]			Sistema Operativo	Tarjeta de red [Mbps]	Servicios de red
			Total	Usada	Libre	Total	Usada	Libre			
SRVUJO	Compaq	Intel Pentium 2E, 1000 MHz	767	540	226	67	55	12	Windows 2000 Server	10/100	Active Directory, DNS, File server
S-McAfee	Clon	Intel Core2Quad CPU Q6600 @ 2.40GHZ	2035	809	1226	465	106	358	Windows 2003 Server	10/100/ 1000	Antivirus
SRVTNC	Clon	Intel Core2Quad CPU Q6600 @ 2.40GHZ	2035	895	1140	298	28	270	Windows 2000	10/100/ 1000	Aplicaciones Thin-Client
Kypus	Nova Devices	Intel Pentium 4 @3.00 GHZ	2048	560	1488	160	n/d	n/d	Kypus Operating System 1.3.0.8	10/100 /1000	Firewall – proxy, DNS, DHCP
SRVBDD / AS-400	IBM	IBM Power5+ @1.9 GHZ	2048	n/d	n/d	140	n/d	n/d	AIX*	2*10/100/ 1000	Base de Datos
SERVIDORES EN GUAYAQUIL											
SRV Video	Digiguard DG0412	n/d	n/d	n/d	n/d	n/d	n/d	n/d	n/d	10/100/ 1000	Video vigilancia

* AIX: Advanced Interactive eXecutive, sistema operativo propietario de IBM para sistemas AS/400

Tabla 2.10 Características de los servidores y sus correspondientes servicios

2.1.2.2.4 Dispositivos Terminales

En Quito y Guayaquil, los dispositivos desde los que se accede a los recursos de la red son computadores portátiles, de escritorio, computadores ligeros (ver sección 2.1.2.4.3) e impresoras de red. Los computadores son de uso personal para tareas de oficina y también para el acceso a los recursos de los servidores. Los dispositivos multimedia, como los parlantes o tarjetas aceleradoras de video, han sido suprimidos en la mayoría de los computadores, por ser innecesarios. Las impresoras de red son accesadas desde cualquier computador o servidor para la emisión de seguros, comprobantes, pólizas, contratos, facturas o de cualquier documento que sea necesario.

Todos los computadores trabajan con procesadores de arquitectura Intel, en alguna de sus diferentes variantes. En el disco duro se almacenan los documentos propios del usuario y las configuraciones particulares de ese computador. Toda información referente al estado de los seguros es almacenada en la base de datos, por lo que no requiere residir localmente en la estación de trabajo. El acceso a la red se da a través de tarjetas NIC (*Network Interface Card*) *Ethernet* típicamente de 10/100 Mbps.

El sistema operativo por el que ha optado la empresa para los dispositivos terminales es *Microsoft Windows*. Alianza adquirió la licencia empresarial para el sistema operativo *MS Windows XP Professional* para los computadores de escritorio, aunque en algunos computadores portátiles se tiene *MS Windows Vista Professional*. Todas las aplicaciones utilizadas en los computadores están basadas en la plataforma de *Microsoft*, por lo que se tiene: *MS Office 2003* para ofimática, *IBM Personal Communications para Windows* como cliente de la base de datos, *MS Internet Explorer 7* como navegador *WEB*, etc. En las tablas 2.11 y 2.12, se resumen el total y las características de los dispositivos terminales de la red de datos.

Dispositivos Terminales Quito				
	PC	Laptop	Thin-Client	Impresora Red
SB	17	3	1	3
PB	6	6	0	1
P1	6	6	0	2
P2	0	0	0	0
PI	4	2	1	1
Total				59
Dispositivos Terminales Guayaquil-Centro				
	PC	Laptop	Impresora Red	
Ala1	7	3	2	
Ala2	15	0	4	
Total				31

Tabla 2.11 *Total de dispositivos terminales de la red en Quito y Guayaquil*

COMPUTADORES		IMPRESORAS	
Característica	Detalle	Característica	Detalle
Marca	Clon / Dell / Sony VAIO / Compaq	Marca	Lexmark T520 / T430
Procesador	Intel / Intel Mobile 2 ~ 3 GHz	Resolución	1200 x 1200 dpi
Almacenamiento	200 ~ 500 GB	Procesador	200 MHz ~ 366 MHz
Memoria	1 ~ 3 GB	Memoria (máx)	264 ~ 269 MB
Tarjeta NIC	10 / 100 Mbps	Tarjeta NIC	10 / 100 Mbps
Sistema Operativo	MS Windows XP Professional / MS Windows Vista Professional		

Tabla 2.12 *Características de los dispositivos terminales*

2.1.2.2.5 *Direccionamiento IP*

Para el direccionamiento IP en Quito y las sucursales se ha tomado el rango de direccionamiento privado clase C 192.168.0.0/24, al cual se lo ha dividido en subredes como se indica en la tabla 2.13.

El direccionamiento IP combina direccionamiento estático y dinámico haciendo uso del servicio proporcionado por DHCP. El servicio de DHCP únicamente se encuentra activado en la red LAN de Quito y contiene el siguiente rango de direcciones IP: 192.168.1.90 - 192.168.1.99 con máscara /24. El direccionamiento estático se encuentra distribuido tanto para los servidores como para las estaciones de trabajo. Las diez primeras direcciones de una subred se encuentran destinadas para los servidores y la última dirección de una subred se encuentra asignada al interfaz del *router* de cada sucursal, como puerta de salida. Las demás direcciones IP se configuran estáticamente en las estaciones de trabajo.

Ciudad	Subred	1era dirección	Última dirección	Dirección de Broadcast	Máscara de subred
Quito	192.168.1.0	192.168.1.1	192.168.1.254	192.168.1.255	255.255.255.0
Cuenca	192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255	255.255.255.0
Guayaquil	192.168.3.0	192.168.3.1	192.168.3.254	192.168.3.255	255.255.255.0
Manta	192.168.4.0	192.168.4.1	192.168.4.254	192.168.4.255	255.255.255.0
Sto. Domingo	192.168.5.0	192.168.5.1	192.168.5.254	192.168.5.255	255.255.255.0
Machala	192.168.6.0	192.168.6.1	192.168.6.254	192.168.6.255	255.255.255.0
TecnoAlianza	192.168.7.0	192.168.7.1	192.168.7.254	192.168.7.255	255.255.255.0
Guayaquil (Ken)	192.168.8.0	192.168.8.1	192.168.8.254	192.168.8.255	255.255.255.0
Milagro	192.168.9.0	192.168.9.1	192.168.9.254	192.168.9.255	255.255.255.0
Advantechsys	192.168.25.0	192.168.25.1	192.168.25.254	192.168.25.255	255.255.255.0

Tabla 2.13 *Direccionamiento IP de la Red Corporativa de Alianza*

Seguros Alianza tiene como ISP (Proveedor de servicio de Internet) y *carrier* a Megadatos S.A, el cual proporciona una dirección IP pública para que Seguros Alianza pueda brindar servicios informáticos al público en general. La dirección IP pública proporcionada es: 64.46.75.92.

2.1.2.3 Red WAN ^[24]

La infraestructura de un *carrier* permite la interconexión entre las LAN de las sucursales de Seguros Alianza, formando así una red WAN. Seguros Alianza lleva un contrato de 4 años con Megadatos S.A. Esta compañía actualmente tiene los permisos de operación de ISP y *carrier* en el territorio nacional. Megadatos S.A. ofrece distintos medios de acceso como: fibra óptica, cables de cobre, enlaces de

microondas, *wimax* y *wifi*, al igual que ofrece distintas tecnologías WAN como: *Frame-Relay* y *MPLS*.

2.1.2.3.1 Equipos WAN

Megadatos S.A. proporciona los equipos de conectividad para la interconexión entre sucursales. Entre los equipos que proporciona se encuentran *modems* DSL y *routers* con *transceivers* para fibra óptica. En las tablas 2.14 y 2.15 se muestran la marca, modelo y ubicación de los dispositivos de conectividad.

ROUTERS				
Cantidad	Marca	Modelo	Ubicación	Empresa
1	Cisco	871	Sistemas	Megadatos
1	Cisco	1811	Sistemas	Megadatos
MODEMS				
Cantidad	Marca	Modelo	Ubicación	Empresa
1	Cisco	575	Sistemas	Megadatos
1	Vulcano		Sistemas	TV-Cable

Tabla 2.14 *Equipos de conectividad WAN QUITO*

ROUTERS				
Cantidad	Marca	Modelo	Ubicación	Empresa
1	Cisco	871	Sistemas	Megadatos
MÓDEMS				
Cantidad	Marca	Modelo	Ubicación	Empresa
1	Cisco	575	Sistemas	Megadatos

Tabla 2.15 *Equipos de conectividad WAN GUAYAQUIL*

Además de los equipos descritos, existe un modem adicional de marca Vulcano perteneciente a la empresa de telecomunicaciones *TvCable*, por el cual Seguros Alianza se conecta a un servidor ubicado remotamente en *Advantechsys*, una filial de Alianza.

2.1.2.3.2 Enlaces WAN

La empresa tiene contratados al momento, ocho enlaces de datos con Megadatos S.A.: dos enlaces de fibra óptica, dos enlaces de microondas y el resto de enlaces con cobre. Los enlaces de Quito y Guayaquil tienen una capacidad de 8192 kbps y 2048 kbps, respectivamente, utilizados para la transferencia de datos y acceso a Internet. Todos los enlaces tienen una compartición de 1:1 o llamados también *clear-channel*. En la tabla 2.16 se muestra el tipo de medio de transmisión, ancho de banda y ciertos parámetros de los enlaces con los que cuenta Seguros Alianza.

Agencia	Últimas millas	Ancho de banda [kbps]	Compartición	Parámetros
Gye principal	Cobre	2048	Clear channel 1:1	CIR 100% BIR 100%
Gye Kennedy	Microonda	256	Clear channel 1:1	CIR 100% BIR 100%
Machala	Cobre	256	Clear channel 1:1	CIR 100% BIR 100%
Quito matriz	Fibra	8192	Clear channel 1:1	CIR 100% BIR 100%
Milagro	Fibra	256	Clear channel 1:1	CIR 100% BIR 100%
Cuenca	Cobre	1024	Clear channel 1:1	CIR 100% BIR 100%
Manta	Microonda	256	Clear channel 1:1	CIR 100% BIR 100%
Santo Domingo	Cobre	256	Clear channel 1:1	CIR 100% BIR 100%

Tabla 2.16 *Enlaces de transmisión de datos y acceso a Internet*

2.1.2.3.3 Acuerdos de Nivel de Servicio ^[5]

Los SLA o acuerdos de nivel de servicio, describen en un contrato el nivel de calidad de un servicio, en este caso de telecomunicaciones, brindado por un proveedor hacia su cliente. Seguros Alianza lleva un contrato vigente con Megadatos S.A. donde se especifica el servicio y las condiciones a cumplir por ambas partes (ver anexo B).

Por parte del operador de servicios se ofrece una disponibilidad de 99.6% al año para los servicios de Internet y última milla. Mensualmente se prevé una disponibilidad del servicio del 98% medido en 30 días de un mes. El tiempo de

respuesta para una falla es de 120 minutos máximo, más el tiempo de desplazamiento de los técnicos a las oficinas del cliente. El soporte técnico que se dispone actualmente es de 24 horas del día, los 7 días de la semana los 365 días del año.

Por parte del cliente se tiene la responsabilidad del mantenimiento y funcionamiento de su red para que el servicio opere en óptimas condiciones. El cliente es responsable del uso que le dé al servicio, es decir, el operador no se hará responsable si terceros interceptan información, esté o no encriptada, así como la transmisión de virus informáticos a través de las redes.

2.1.2.4 Servicios y Aplicaciones de Red

Los siguientes servicios son los que se prestan actualmente dentro de la red corporativa de Alianza de Seguros para uso de sus empleados. El servicio WEB es accesible para el público a través de Internet pero no forma parte de la red corporativa de Alianza.

- Servicio de Bases de Datos (SRVBDD)
- Servicio de Antivirus (S-McAfee)
- Servicio de Aplicaciones (SRVTNC)
- Servicio de Escritorio Remoto
- Servicio de Correo Electrónico (Kypus)
- Servicio de DNS
- Servicio de DHCP
- Servicio WEB
- Servicio de Directorio Activo
- Servicio de Video Vigilancia (SRV Video)

En cada servicio se especifican las aplicaciones utilizadas para su funcionamiento.

2.1.2.4.1 Bases de Datos ^{[4][6][7][8][9]}

Se trata del servicio de red más importante para la empresa ya que concentra toda su información. Mantiene de forma ordenada los datos y permite relacionarlos para obtener información detallada de: clientes, pólizas de seguros, pólizas de reaseguros, nómina del personal, ingresos, gastos en productos, bienes y servicios de la empresa, etc. A la base accede la mayoría de empleados para la realización de sus actividades diarias.

La plataforma que soporta el servicio de bases de datos está conformada por: un servidor IBM AS/400, ubicado en la matriz de la empresa, el sistema operativo AIX y el sistema de manejo de bases de datos DB-2. Tanto el *hardware* como el *software* son propietarios de IBM. Los usuarios acceden al servicio mediante un emulador de terminal específico para este servicio, desde cualquier sucursal, a través de la red corporativa de la empresa.

El sistema AIX, similar a UNIX, brinda todas las funcionalidades necesarias de red y almacenamiento para la base DB2. DB2 es la marca registrada de IBM para su sistema de gestión de bases de datos relacionales, cuyo lenguaje de consultas es el SQL (*Structured Query Language*). El puerto en el que escucha este servicio por defecto es el 523, para aceptar las conexiones de los clientes; sin embargo, este puerto es poco utilizado, puesto que el servidor es accedido vía *Telnet* (puerto 23) para las consultas habituales.

El *software* cliente es el *Personal Communications iSeries Access para Windows, Programa de estación de trabajo versión 5.7*. Éste es un completo *software* para la administración del servidor AS/400 de forma remota, mediante conexión de red. Incluye un emulador de terminal que se conecta vía *Telnet* al servidor. Cada usuario tiene a disposición una cuenta para poder acceder al servidor dependiendo de sus funciones; esto es, existen cuentas de administrador y cuentas de usuario regular.

Una de las tareas más comunes que se realizan mediante la base de datos es la emisión de pólizas. La orden de impresión de las pólizas se envía desde el servidor a cualquier impresora dentro de la red corporativa.

Además del servidor principal de base de datos, existe un segundo servidor AS/400 remoto. Este servidor forma parte de Tecno Alianza, una rama de Alianza de Seguros para el manejo del SOAT.

El soporte al servidor de bases de datos lo realiza directamente IBM Ecuador, mediante contrato de soporte anual.

2.1.2.4.2 *Antivirus* ^{[10]-[14]}

Debido a la proliferación y expansión de *software* malicioso y virus en la red, que pueden provocar daños a información importante, se ha elegido como primera protección a la *suite* de antivirus *McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.7i*. La instancia principal del antivirus reside en un servidor dedicado de la matriz. Además, se cuenta con repositorios en cada una de las sucursales y agentes *McAfee Agent 4.5* en cada computador y servidor compatible. La figura 2.8 ilustra el esquema de trabajo del servicio de antivirus en la red empresarial.

El servidor antivirus principal tiene la función de descargar actualizaciones, bases de datos sobre virus y parches oficiales directamente de Internet. Los repositorios consultan al servidor principal para sus respectivas actualizaciones y los agentes bajan estas actualizaciones a cada equipo terminal de la red en intervalos de 60 minutos. Con esto se protege a cada computador de *software* malicioso y se minimiza el uso de los recursos de red.

2.1.2.4.3 *Servicio de Aplicaciones* ^{[15]-[18]}

El servicio de aplicaciones se introdujo como un proyecto piloto en Alianza para minimizar costos y facilitar la administración de los equipos. Consiste en un

servidor con los recursos suficientes (procesamiento, memoria y almacenamiento) para albergar un número de aplicaciones. El acceso se realiza a través de *Thin-Clients* o computadores ligeros con capacidades de procesamiento mínimas, pero con las funciones de red necesarias para la conexión con el servidor.

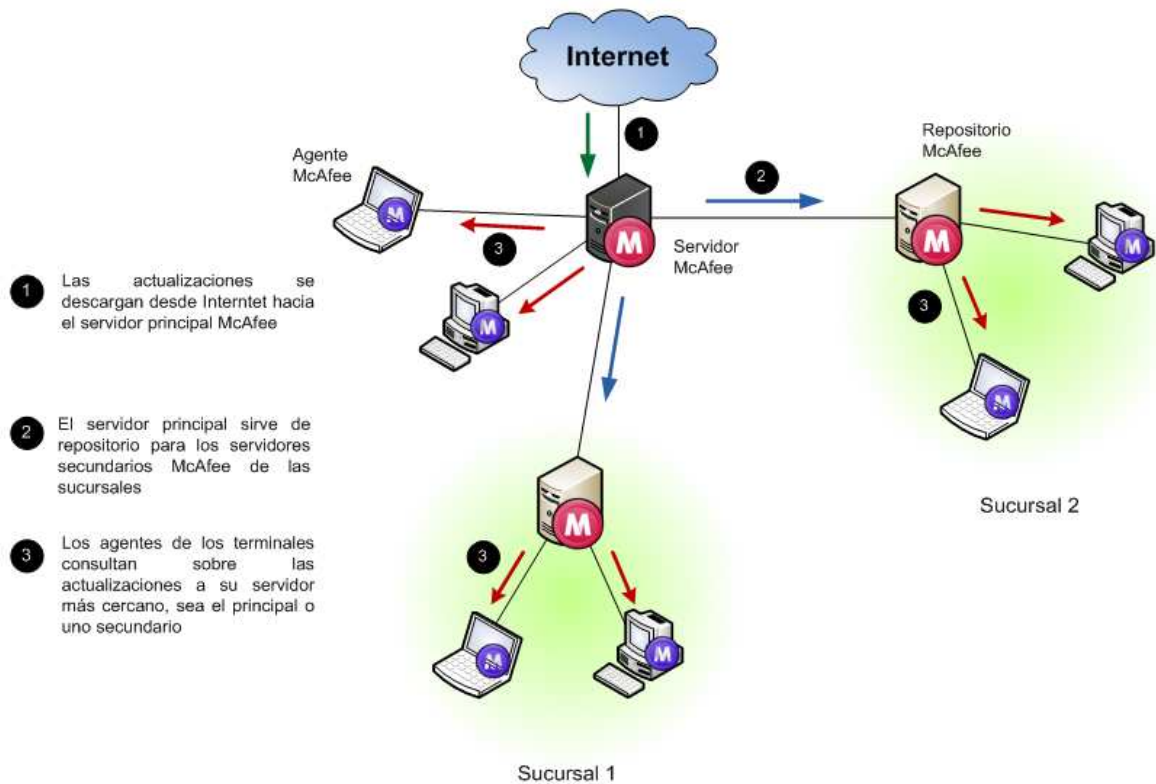


Figura 2.8 Funcionamiento del servicio de antivirus McAfee en Alianza

En la matriz de Alianza se tiene un clon o computador de propósito general como servidor de terminales y dos clientes *Thin-Client* de marca Kypus. En conjunto, el servidor y los terminales representan una fracción del costo de tener tres computadores personales y sus respectivas licencias de *software*. Anteriormente se tenían otros *Thin-Client* en la sucursal de Milagro en proceso de pruebas. El objetivo era utilizar terminales de este tipo en todas las localidades remotas en vez de computadores personales. Este proyecto no se llevó a cabo debido a que los enlaces WAN no presentaban las condiciones necesarias para que los clientes trabajen correctamente con las aplicaciones del servidor de Quito.

Este servicio se centra en el uso del programa *XP Unlimited – Empresarial 2.2* para *MS Windows XP*, que “corre” en el servidor SRVTNC. *XP Unlimited* hace que las aplicaciones del servidor estén disponibles para los clientes de la red. La configuración actual del servicio designa al puerto 3390 para aceptar conexiones y utiliza el servicio de directorio activo para el acceso de los usuarios. Las conexiones se realizan mediante el protocolo de escritorio remoto MSRDP (*Microsoft Remote Desktop Protocol*).

Este servicio está destinado para que las aplicaciones de productividad instaladas en el servidor, como el cliente de base de datos o MS Office, sean accesibles en los equipos *Thin-Client*.

2.1.2.4.4 Escritorio Remoto ^[19]

Mientras que el servicio de terminal permite el control total o parcial de un sistema remoto mediante comandos de texto, el servicio de escritorio remoto provee las mismas funciones pero en modo gráfico. Gracias a las facilidades de uso que presenta una interfaz gráfica para el usuario, el servicio de escritorio remoto forma parte de la mayoría de servidores y computadores actuales.

Las aplicaciones de escritorio remoto usadas en Alianza son el servidor VNC Server 4.0 y el cliente WinVNC 3.3.7. El servidor escucha las peticiones de conexión en los puertos 5900 y 5800. El segundo puerto se encuentra activo para las conexiones realizadas desde interfaces WEB. Para que el cliente se conecte se necesita la dirección IP o nombre del host remoto y las credenciales de usuario para la autorización de acceso.

Este servicio es utilizado con regularidad por el personal del Departamento de Sistemas de Alianza. Con este servicio se realizan tareas de administración como la configuración de los servidores y estaciones de trabajo, tal como si se estuviera al frente del equipo administrado. Todo equipo que vaya a ser administrado remotamente necesita tener instalado el *software* servidor de escritorio remoto.

Si bien este servicio resulta de utilidad por la facilidad de manejar interfaces gráficas, puede no resultar conveniente en situaciones de congestión de la red, o cuando se tienen enlaces de baja capacidad.

2.1.2.4.5 *Correo electrónico*^[14]

El correo electrónico es uno de los servicios principales que se puede encontrar en una red. Proporciona un fácil intercambio de texto o archivos entre los usuarios de la misma red, o de redes diferentes. En Seguros Alianza se dispone de un servicio de correo electrónico activado en el servidor Kypus. Este servicio se implementa a través del uso del protocolo POP3 y SMTP. Se dispone del *software* servidor *Sendmail*, desarrollado para Linux.

2.1.2.4.6 *Compartición de Archivos*

En la empresa se manejan documentos que son utilizados por varios departamentos. Se requería la optimización de recursos y de tiempo para que el personal acceda a dichos documentos. Así nació la necesidad de un mecanismo de compartición de archivos.

La creación de unidades lógicas de disco en el servidor central de Quito (SRVUIO) y la compartición de las mismas, permitieron el acceso a documentos importantes entre departamentos a los empleados. Las unidades de compartición son: E:\, G:\, K:\ y L:\; con un total de 36 GB para este servicio. Para Guayaquil se plantea la posible creación de un servidor de este tipo.

Con la utilización del sistema operativo para servidor, Windows 2000 Server, y estaciones de trabajo con Windows XP, se maneja el protocolo CIFS (*Common Internet File System*) para la compartición de archivos a través de la compartición de las unidades lógicas del servidor.

2.1.2.4.7 WEB

Actualmente el servicio WEB está siendo desarrollado por parte del Departamento de Sistemas, para la cotización de pólizas de seguros y SOAT, emisión de seguros, consultas de pólizas para los clientes, entre otras aplicaciones. El servicio WEB será una alternativa a la consulta de la base de datos mediante terminales por parte del personal de Seguros Alianza.

Adicionalmente se tiene una página WEB con la siguiente url: <http://www.segurosalianza.com> que se encuentra alojada en un servidor externo de la empresa *Network Solutions* en Estados Unidos, la cual presta los servicios de *hosting* a Alianza.

2.1.2.4.8 DNS ^{[25][26]}

En toda red es fundamental la traslación de direcciones IP a nombres fáciles de recordar y viceversa, para la identificación de algún recurso. Por ello se creó el servicio de DNS. Seguros Alianza tiene un servidor DNS local, únicamente para Quito, en el servidor principal (SRVUIO). Este servidor es de tipo caché y recursivo, es decir que cualquier dirección que no la pueda resolver a un nombre, la enviará a otro servidor DNS externo pre configurado. Cuando el servidor DNS externo resuelve la dirección, envía la respuesta al servidor DNS de Alianza y éste almacena la respuesta en su memoria para posteriores peticiones, con lo que se disminuye el tiempo de respuesta. Los servidores DNS externos forman parte del servicio proporcionado por el *carrier* o ISP, en este caso, MEGADATOS S.A.

Se tiene configurado otro DNS en el servidor Kypus para la resolución de nombres en el resto de sucursales.

Alianza cuenta con el dominio *segurosalianza.com*, hospedado en los servidores de la empresa *Network Solutions* en Estados Unidos. Los servidores se identifican como: ns4.accessinter.net y ns-gye.accessinter.net con dirección IP 64.46.64.254 y 64.46.78.130, respectivamente.

2.1.2.4.9 DHCP

Con la generación de un área de trabajo para los *brokers* de seguros, y la dificultad en la configuración de sus equipos portátiles por parte de un técnico del Departamento de Sistemas, se añade a la red el servicio de DHCP, activo en el servidor Kypus. Con este servicio se realiza la configuración dinámica de direcciones IP. Es importante mencionar que este servicio sólo se encuentra activado para la red de Quito.

El rango de direcciones utilizado para DHCP va desde 192.168.1.90 a 192.168.1.99. Además se configura el *default gateway* como 192.168.1.1 y el servidor DNS con 192.168.1.5 con DNS alternativo 192.168.1.1.

2.1.2.4.10 Firewall^[14]

El *firewall* es un dispositivo de seguridad importante dentro de una red. Éste bloquea los accesos no autorizados a los recursos de la red. El *firewall* puede ser implementado tanto en *hardware*, *software* o la combinación de ambos. Controla los paquetes entrantes o salientes, siguiendo las reglas de seguridad determinadas por el administrador de la red.

En la empresa se cuenta con un *firewall* implementado en *hardware* más un *software* desarrollado para Linux. El servidor lleva por nombre *Kypus Appliance*, proporcionado por la empresa *Nova Devices*, siendo éste un multi-servidor con varios servicios de red como: DHCP, DNS, mail-server, WEB-server, VPN-server, entre otros.

El *firewall* se encuentra trabajando con filtrado de paquetes y realiza funciones de un *proxy* como: filtrado de páginas WEB o filtrado dependiente del contenido, caché de páginas WEB y translación de direcciones (NAT).

2.1.2.4.11 Directorio Activo ^[20]

El servicio de directorio se relaciona estrechamente con las características organizacionales de una empresa: maneja información personal y de contacto del recurso humano más la información de los recursos de red. En este entorno, la información de directorio se puede usar para implementar las políticas organizacionales de la empresa y también como un mecanismo de seguridad. La utilización de los recursos de red se permite únicamente si el usuario cumple con el perfil adecuado, basado en la información del directorio.

Alianza cuenta con el servicio de Directorio Activo en el servidor SRVUIO, basado en *MS Active Directory* sobre una plataforma *MS Windows 2000*. Este servidor contiene toda la información de los usuarios de la red de Quito y en particular sólo permite el acceso a los recursos de red basados en sistemas operativos *Microsoft* compatibles. Su uso más común es para el acceso al servidor de archivos, escritorio remoto y acceso a las cuentas de las estaciones de trabajo.

A excepción de Quito, la información de directorio y el acceso a las cuentas del resto de sucursales, se maneja a través del servidor KYPUS, mediante el directorio LDAP (*Lightweight Directory Access Protocol*) sobre una plataforma Linux.

2.1.2.4.12 Video – Vigilancia ^[21]

El sistema de video–vigilancia surge de la necesidad de proporcionar mayor seguridad para las oficinas de Guayaquil. Para el efecto, se utiliza un servidor de video de marca *DIGIGUARD DVR SERIES H.264*. Tiene cuatro canales de entrada del tipo coaxial, para cámaras de video, y un puerto de acceso a la red LAN. Este servidor establece comunicación con cuatro cámaras ubicadas en puntos estratégicos de las oficinas. Usando cualquier navegador WEB con soporte para contenido multimedia, se puede acceder a las cámaras y visualizar en tiempo real lo que está sucediendo, al apuntar a la dirección IP 192.168.3.14,

en el puerto 800. El monitoreo está habilitado únicamente dentro de la red corporativa de Alianza.

2.1.2.5 Enrutamiento

La red corporativa de la empresa contiene un esquema de enrutamiento estático. Estas rutas definen el encaminamiento de cada paquete y se encuentran configuradas en el servidor Kypus, mostradas en la tabla 2.17. Adicionalmente, en la figura 2.9, se muestran los equipos de conectividad con sus respectivas direcciones IP.

Interfaz	Subred	Máscara de subred	Default Gateway	Ubicación
LAN 1	192.168.2.0	255.255.255.0	192.168.1.254	Cuenca
LAN 1	192.168.3.0	255.255.255.0	192.168.1.254	Guayaquil
LAN 1	192.168.4.0	255.255.255.0	192.168.1.254	Manta
LAN 1	192.168.5.0	255.255.255.0	192.168.1.254	Sto. Domingo
LAN 1	192.168.6.0	255.255.255.0	192.168.1.254	Machala
LAN 1	192.168.7.0	255.255.255.0	192.168.1.254	Tecno Alianza
LAN 1	192.168.8.0	255.255.255.0	192.168.1.254	Guayaquil Centro
LAN 1	192.168.9.0	255.255.255.0	192.168.1.254	Milagro
LAN 1	192.168.25.0	255.255.255.0	192.168.1.8	Advantechsys

Tabla 2.17 *Planeación de direccionamiento IP para enrutamiento*

Como se puede visualizar en la figura 2.9, en el *router* UIO se tienen dos enlaces que se conectan a la red LAN de Quito, uno a través del servidor Kypus y el otro a un *switch* del segmento LAN. El enlace que se conecta al servidor Kypus pertenece a una subred pública 64.46.75.88/29 configurada por el proveedor de servicios. El segundo enlace está configurado en otra interfaz del *router* UIO con la dirección privada 192.168.1.254/24.

Para entender el funcionamiento de las rutas en la red corporativa de Alianza es necesario separar los escenarios de la matriz y de las sucursales, descritos a continuación.

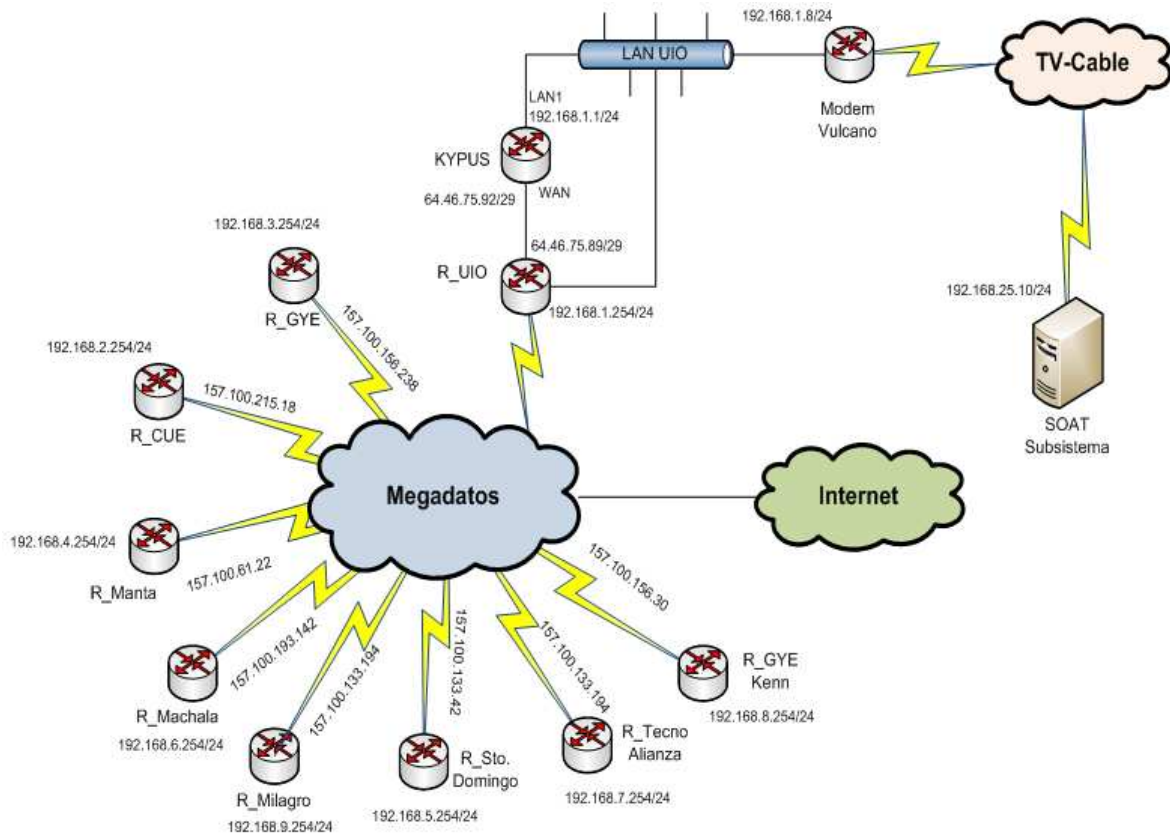


Figura 2.9 Configuración actual de las direcciones IP en la Red Corporativa de Alianza

Todas las estaciones de trabajo, servidores y dispositivos terminales de la red LAN Quito tienen como *default gateway* a la IP 192.168.1.1, interfaz del servidor KYPUS denominada “LAN1”. Este servidor contiene todas las rutas de la red corporativa de la empresa, configuradas de forma estática.

Una petición hecha desde la red LAN Quito puede ser dirigida a cualquier dispositivo dentro o fuera de esta red. Si es una petición para la red LAN Quito, ésta alcanza directamente al dispositivo solicitado sin ningún salto. Si es una petición para un dispositivo ajeno a la red LAN Quito, ésta pasa al servidor Kypus y puede ser redirigida a las sucursales o hacia el Internet. Si son peticiones hacia las sucursales, éstas son redirigidas hacia la interfaz del *router* UIO, cuya dirección IP es 192.168.1.254/24, para ser transportadas hacia su destino por la red corporativa, haciendo uso de los servicios del *carrier*. Cuando son peticiones

hacia Internet salen a través de la interfaz WAN del servidor Kypus con la IP pública y son enrutadas por el *router* UIO por el camino más adecuado.

Todas las sucursales tienen una configuración similar de enrutamiento. En cada sucursal se utiliza la última dirección IP válida como *default gateway*, por ejemplo, en Guayaquil (Centro) el *default gateway* es la interfaz con dirección IP 192.168.3.254/24. Al igual que en Quito, las peticiones internas no necesitan ningún salto para alcanzar al dispositivo requerido de manera directa. Por otra parte, las peticiones externas no tienen diferenciación, sean a otras sucursales o hacia Internet, todas son enviadas a Quito, allí se decidirá su destino según las rutas descritas en la tabla 2.17.

2.1.2.6 Análisis de Tráfico

Para el análisis de tráfico, basado en la utilización del ancho de banda de los enlaces, se activó el servicio SNMP en los *routers* y servidores accesibles. Además, en el servidor de aplicaciones, se instaló el programa *PRTG (Paessler Router Traffic Grapher) Network Monitor* que contiene una serie de herramientas para obtener el tráfico y otros datos en una red IP. Los datos de tráfico fueron recolectados en el periodo de Febrero a Mayo de 2010.

Los enlaces monitoreados y analizados a continuación son: el enlace WAN de Quito, que corresponde a la sumatoria de todos los enlaces de las sucursales y la salida a Internet; el enlace WAN de Guayaquil (centro), y los enlaces locales de los servidores en Quito, por representar el mayor volumen de tráfico de la red.

2.1.2.6.1 Enlace WAN Quito

El enlace fundamental para la red corporativa de Alianza de Seguros es el enlace WAN de Quito. Este enlace simétrico dedicado tiene una capacidad de 8192 kbps. Por él cruza tanto el tráfico de las sucursales como el de Internet. El tráfico que cruzó durante el periodo de monitorización se muestra en la figura 2.10.

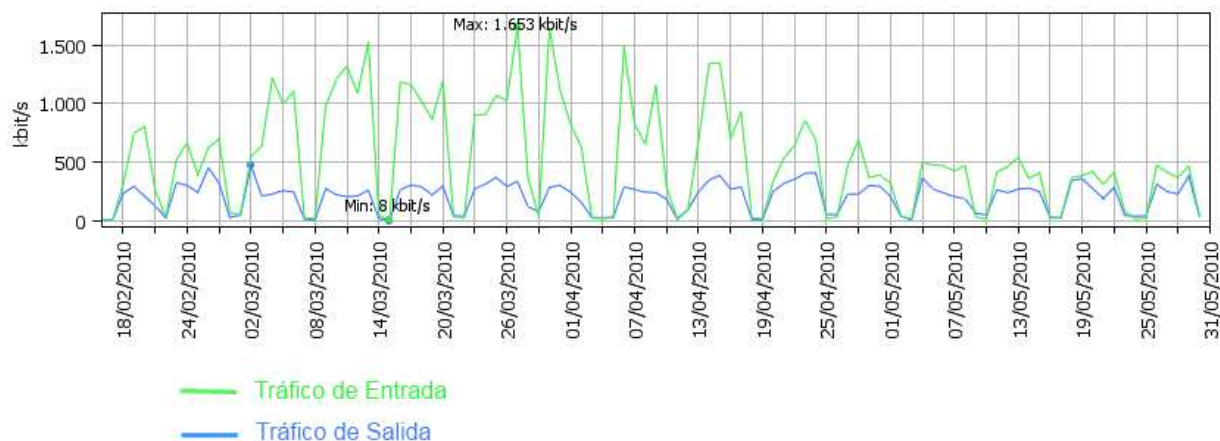


Figura 2.10 *Tráfico de entrada y salida del enlace WAN Quito, periodo Febrero-Mayo 2010*

En la figura 2.10 se puede apreciar la tendencia de tráfico entrante y saliente, donde predomina el tráfico de entrada. Durante el periodo analizado se puede apreciar un fuerte flujo de entrada de datos entre los meses de febrero y abril, mientras que el tráfico de salida mantiene un patrón que se repite constantemente.

Al final del periodo observado casi se iguala el tráfico entrante con el saliente. De este periodo se ha procedido a verificar cuál es la semana de mayor tráfico para el enlace WAN de Quito, obteniéndose los resultados de la tabla 2.18.

De la tabla 2.18 se obtuvo que la semana con mayor tráfico fue la comprendida entre el 8 y 14 de marzo de 2010, cuya caracterización y valores se representan en la figura 2.11 y en la tabla 2.19 respectivamente.

En la figura 2.11 se muestra claramente que el tráfico es generado en el horario de trabajo de Alianza de Seguros esto es, de lunes a viernes, de 8:00 a 20:00. El trabajo en fines de semana es inusual, por lo tanto el tráfico es cercano a cero. En general, el tráfico de entrada en este enlace es mayor al de salida, y en la semana analizada esta relación es aún mayor, siendo aproximadamente de 6 a 1.

Mes	Semana			Volumen de Datos [GB]	
				Entrada	Salida
Febrero	15/02/2010	-	21/02/2010	21.85	9.13
	22/02/2010	-	28/02/2010	30.50	17.40
Marzo	01/03/2010	-	07/03/2010	45.73	14.51
	08/03/2010	-	14/03/2010	61.93	12.16
	15/03/2010	-	21/03/2010	55.16	14.79
	22/03/2010	-	28/03/2010	59.96	18.05
	29/03/2010	-	04/04/2010	43.08	10.86
Abril	05/04/2010	-	11/04/2010	41.67	12.27
	12/04/2010	-	18/04/2010	49.50	15.35
	19/04/2010	-	25/04/2010	30.81	18.35
	26/04/2010	-	02/05/2010	23.21	13.22
Mayo	03/05/2010	-	09/05/2010	24.07	14.05
	10/05/2010	-	16/05/2010	22.67	13.74
	17/05/2010	-	23/05/2010	20.15	15.57
	24/05/2010	-	30/05/2010	18.32	13.25

Tabla 2.18 *Volumen de tráfico semanal enlace WAN Quito tomado entre Febrero y Mayo de 2010*

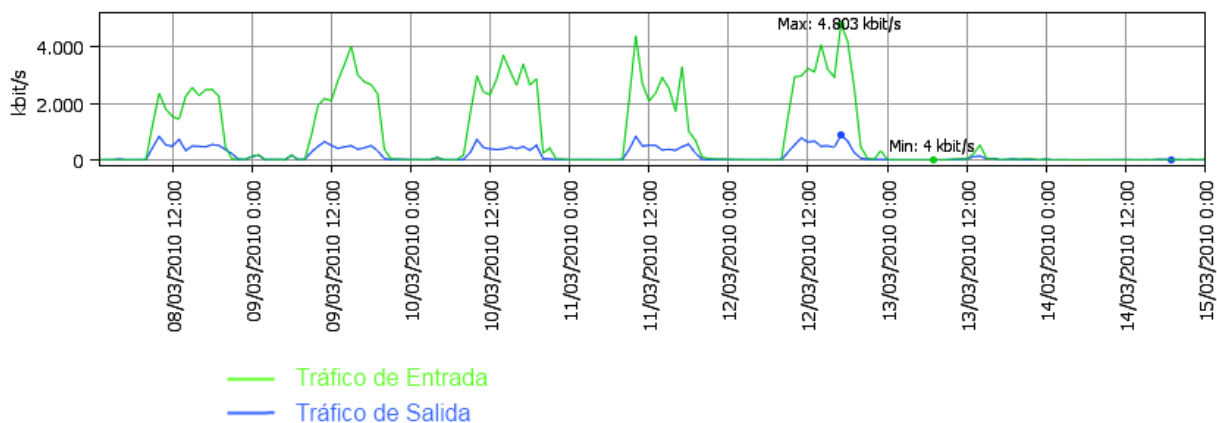


Figura 2.11 *Semana de mayor tráfico del enlace WAN Quito del 8 al 14 de marzo 2010*

La tabla 2.19 contiene los valores máximos de velocidad de transmisión de entrada y salida, así como el promedio del diez por ciento de las velocidades más altas, de manera que se puede constatar que el enlace no tiende a saturarse.

Tráfico	Capacidad	Velocidad Máxima	Promedio del 10% de Valores Máximos
Entrada [kbps]	8192	4803	3537
Salida [kbps]	8192	877	658

Tabla 2.19 Velocidad máxima de entrada y salida del Enlace WAN Quito

El canal WAN de Quito tiene una capacidad de 8192 kbps. Está formado por la suma de las capacidades de los enlaces de cada sucursal, 3328 kbps en total más la diferencia, utilizada para salir a Internet (en el anexo C.1 se muestra las gráficas de las demás sucursal en la semana de mayor tráfico). Cuando el enlace no está ocupado con tráfico de las sucursales, puede ser usado en toda su capacidad para tráfico de Internet. De esta manera se puede concluir que el enlace está sobredimensionado.

2.1.2.6.2 Enlace WAN Guayaquil-Centro

El enlace WAN de Guayaquil-Centro es el segundo de mayor capacidad de la red corporativa de Alianza de Seguros, con 2048 kbps. Guayaquil-Centro es la sucursal que genera mayor tráfico en la red corporativa, después de Quito, y éste tiene su propio patrón, representado en la figura 2.12, cuya semana de mayor trabajo es diferente a la obtenida en el enlace WAN de Quito, del 22 al 29 de marzo 2010.

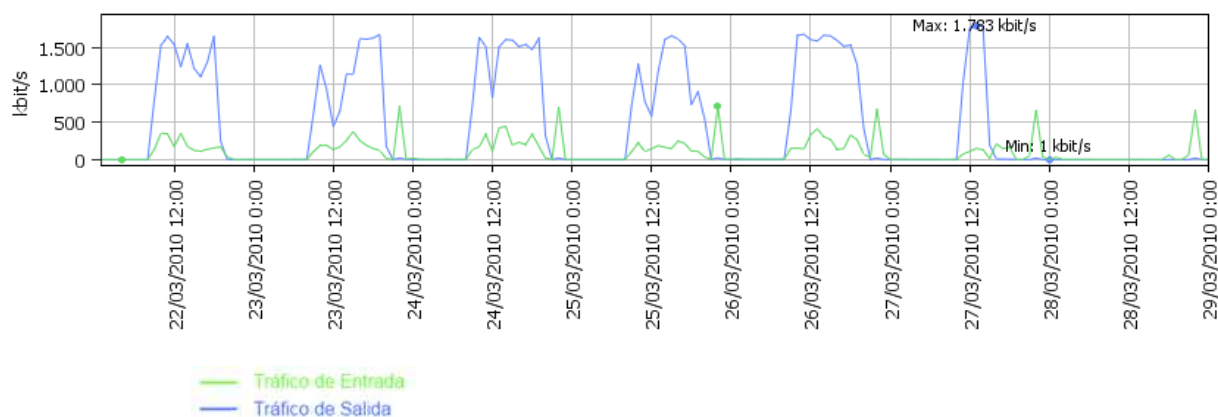


Figura 2.12 Semana de mayor tráfico del enlace WAN Guayaquil del 22 al 29 de marzo 2010

La semana de mayor tráfico para este enlace se ha escogido en base al tráfico de salida por dos razones: debido a que es mayor que el tráfico de entrada y a que la capacidad del enlace es simétrica en ambos sentidos. Al igual que en Quito, el canal se ocupa prácticamente sólo entre semana en horario de oficina, con escasas excepciones. La tabla 2.20 resume los valores máximos y promedio del enlace WAN de Guayaquil, donde también se puede apreciar que el canal no llega a saturarse.

Tráfico	Capacidad	Velocidad Máxima	Promedio del 10% de Valores Máximos
Entrada [kbps]	2048	709	481
Salida [kbps]	2048	1783	1664

Tabla 2.20 *Velocidad máxima de entrada y salida del enlace WAN de Guayaquil*

2.1.2.6.3 Enlaces hacia los servidores

Los servidores son una parte fundamental de la red corporativa de la empresa, marcando una importancia en el análisis de tráfico de cada servidor. Para este análisis se monitoreó todas las interfaces físicas de cada servidor, tomando el mismo periodo de recolección de datos de tráfico anterior, febrero a mayo de 2010, y siguiendo el mismo procedimiento usado para el análisis de los enlaces anteriores.

Servidor	Intervalo	Traffic In [Byte]	Traffic Out [Byte]
McAfee	26/04/2010 - 02/05/2010	4847886	15638830
SRVUIO	26/04/2010 - 02/05/2011	8576803	1995173
AS-400	Lineth	01/03/2010 - 07/03/2010	681008
	Ethlocal	19/04/2010 - 25/04/2010	808185
Kypus	ETH0	08/03/2010 - 14/03/2010	71007019
	ETH1	12/04/2010 - 18/04/2010	4089537
Thin-Client	19/04/2010 -25/04/2010	1214983	19714150

Tabla 2.21 *Volumen de tráfico de los servidores*

En la tabla 2.21 se muestra un resumen de la semana con mayor tráfico en los enlaces hacia cada uno de los servidores y se detalla la cantidad de tráfico que cursó durante esa semana. En la tabla 2.22 se puede observar la velocidad máxima de entrada y salida de cada uno de los enlaces hacia los servidores. En el anexo C.2 se muestra la caracterización gráfica de cada uno de los servidores en su semana de mayor tráfico.

Servidor		Velocidad Máxima		Promedio 10% Máximo		Velocidad del puerto
		Entrada [kbps]	Salida [kbps]	Entrada [kbps]	Salida [kbps]	[Mbps]
McAfee		868	2853	375	1267	1000
SRVUIO		16370	524	1042	154	100
AS-400	Lineth	91	2244	49	739	1000
	Ethlocal	128	4641	60	1341	1000
Kypus	ETH0	14348	3478	6436	2430	1000
	ETH1	5064	615	3584	335	1000
Thin-Client		383	13654	84	2259	1000

Tabla 2.22 Velocidad máxima de los enlaces hacia los servidores

El tráfico de los servidores se caracteriza por ser generado en horario de trabajo, lunes a viernes, de 8:00 a 20:00, con excepción del tráfico generado por el servidor McAfee, que requiere de actualizaciones desde Internet por lo que su horario se extiende a los días sábados y domingos. De la tabla 2.22, se tienen las siguientes observaciones:

- El servidor *McAfee* soporta mayor tráfico de salida que de entrada, siendo sus valores máximos: 2853 kbps de salida respecto a 868 kbps de entrada. El tráfico que soporta, provocado tanto por la descarga de actualizaciones y peticiones de los agentes, se produce a lo largo de la jornada laboral de manera periódica con un promedio de 1267 kbps de salida; mientras el resto del tiempo el tráfico es mínimo y constante manteniéndose en 4 kbps, según lo mostrado en la figura C.12 del anexo C.2.

- El servidor UIO soporta como servicios: el almacenamiento de archivos, Active Directory y DNS. Su flujo promedio de entrada de datos, 1042 kbps, es mayor que el de salida, 154 kbps. El tráfico es provocado principalmente por la transferencia de archivos desde el servidor hacia los PC's y viceversa. El servidor de archivos trabaja bajo demanda, por lo tanto lo hace sólo en jornada laboral. El porcentaje de utilización de la capacidad de entrada y de salida no llega a 1%.
- Para el servidor de Base de datos AS-400 se tiene que el tráfico de salida es mayor al de entrada. El tráfico de salida generado principalmente por las consultas que se realizan a la base de datos que en promedio no sobrepasan los 1341 kbps, utilizando aproximadamente el 1% de la capacidad de su enlace.
- El servidor de aplicaciones soportó un tráfico de salida máximo de 13654 kbps y un tráfico de entrada máximo de 383 kbps. Se puede mencionar que el tráfico de salida en promedio es mayor al de entrada, producido por las descargas de aplicaciones desde este servidor a los clientes *Thin-Client*.
- Finalmente se tiene el servidor Kypus donde residen principalmente los servicios de correo electrónico y de *firewall-proxy* de la red. La mayor parte de peticiones se dirigen hacia el Internet, observándose valores promedio de entrada de 6 Mbps y 3 Mbps, y de salida de 2 Mbps a 0,3 Mbps.

2.1.2.6.4 Protocolos^{[20] [22] [23] [27]}

Para el análisis de la utilización de los protocolos dentro de la red, se utilizó el *software Colasoft Capsa 6.9*. Se analizó tanto el tráfico generado por los servidores como el generado por los clientes. En la figura 2.13 se muestra el porcentaje de utilización de los diferentes protocolos de la red en un día de trabajo.

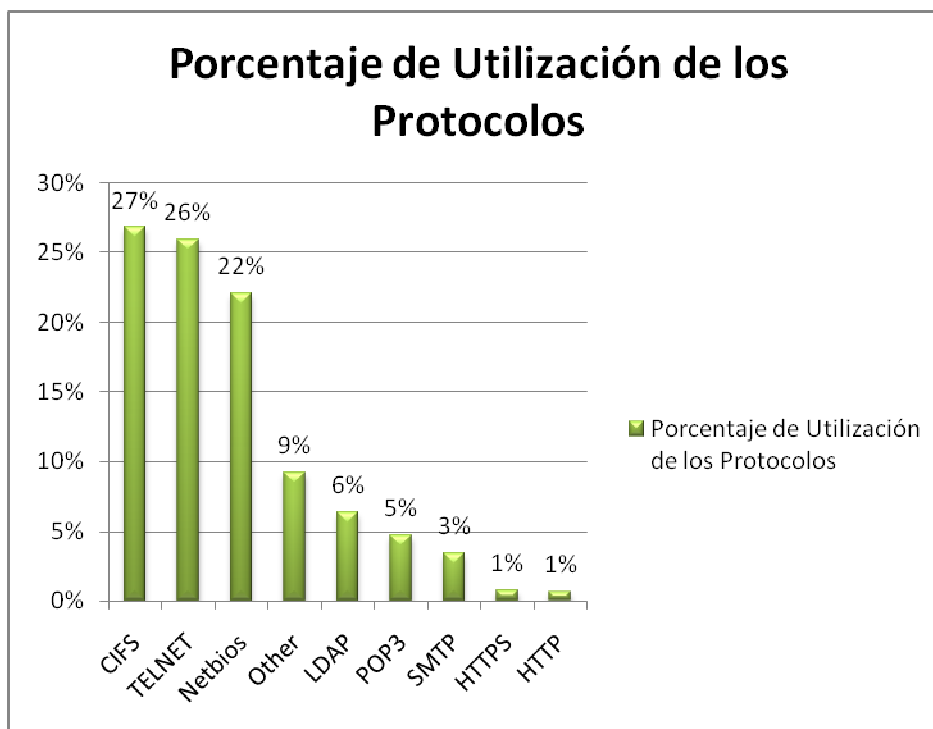


Figura 2.13 Porcentaje de utilización de los protocolos

Como se puede observar, los protocolos de mayor uso son: CIFS, *Telnet* y *NetBIOS*; que en son utilizados para la conexión con el servidor de archivos, base de datos y servidores *Microsoft*, respectivamente. El protocolo *NetBIOS* puede ser deshabilitado en un ambiente con LDAP y DNS. Dentro de los protocolos referidos como **Other** se encuentran las conexiones hacia el servidor *McAfee*, el tráfico DHCP, consultas DNS, etc. Se observa además, que los protocolos HTTP y HTTPS son de muy baja utilización, lo cual se debe a que las políticas de uso de la red sólo permiten acceso a ciertas páginas permitidas en la empresa.

Es importante mencionar que el servidor de aplicaciones utiliza el protocolo MSRDP (*Microsoft Remote Desktop Protocol*) para la comunicación con sus clientes, el mismo que genera el 95% del tráfico total de este servidor.

2.1.3 ANÁLISIS DE LA RED TELEFÓNICA

Uno de los primeros y más tradicionales servicios de telecomunicaciones existentes en cualquier empresa es el de Telefonía. Para este servicio, Alianza

hace uso de dos sistemas: una centralita o PBX en cada sucursal para el uso interno, y la PSTN para llamadas externas a través de la infraestructura nacional de la CNT. Mediante la PSTN se tiene la interconexión entre sucursales, interconexión con otras operadoras (nacionales e internacionales, fijas y celulares) lo que posibilita contactarse con clientes o miembros de la empresa fuera de las oficinas.

Además de los servicios de la CNT, Alianza cuenta con un plan celular empresarial con la empresa Movistar para las llamadas celulares, el cual se mantiene por cuestiones operativas y de costos.

2.1.3.1 Infraestructura Telefónica en Quito y Guayaquil

Las dos principales oficinas de Alianza, en Quito y Guayaquil-centro, cuentan con centralitas, o PBX, y líneas troncales de la CNT. En las PBX se concentran las troncales y las extensiones telefónicas, conectadas a través de cables multipar. Entre los terminales telefónicos se encuentran: teléfonos analógicos y digitales, faxes y dispositivos *datafast*, distribuidos en los diferentes departamentos.

La infraestructura telefónica actual de Alianza, en Quito y Guayaquil, tiene un tiempo de vida aproximado de 10 años. En este tiempo se han actualizado las PBX y se han añadido tarjetas de expansión para cubrir la capacidad requerida. Estas actualizaciones se han dado en la medida que las características de los equipos lo han permitido.

2.1.3.1.1 Central Telefónica de Quito ^{[29][30]}

En Quito, se cuenta con dos PBX de tipo propietario, marca Panasonic, de la serie KX-TD1232. Estas centralitas telefónicas son híbridas, es decir, soportan troncales y extensiones que pueden ser analógicas y digitales.

Cada PBX KX-TD1232 tiene una capacidad máxima para 32 extensiones telefónicas de tipo SLT (*Single Line Telephone*), 6 interfaces BRI (*Basic Rate Interface*) o 64 estaciones portables DECT (*Digital Enhanced Cordless Telecommunications*), como terminales telefónicos; y 12 troncales analógicas, 6 interfaces BRI o 1 interface PRI (*Primary Rate Interface*) para líneas públicas. Además, soporta los siguientes módulos para expansión y ampliación de capacidades:

- **Tarjeta de Interconexión de Sistema.** Con esta tarjeta se pueden interconectar dos PBX Panasonic KX-TD1232 para hacerlas trabajar como una, y así duplicar la capacidad, tanto de extensiones como de troncales.
- **Módulos de expansión.** Permiten incrementar la capacidad inicial de la PBX añadiendo tarjetas para troncales y extensiones.
- **Tarjeta Contestadora DISA (*Digital Inward System Access*).** Con esta tarjeta se añaden funciones de contestadora automática a la PBX y permite a quien llama desde fuera acceder a algunas funciones de la PBX, como por ejemplo, listar extensiones internas.

Otros módulos pueden ser adquiridos para aumentar funcionalidades como la interconexión con redes ISDN o el soporte de dispositivos inalámbricos DECT.

La figura 2.14 representa las dos PBX Panasonic KX-TD1232 con sus módulos extra para extensiones y líneas troncales. La PBX 1 está al máximo de su capacidad con 2 módulos de extensiones y uno de líneas troncales, mientras que la PBX 2 tiene espacio para un módulo extra, sea para extensiones o troncales.

La figura 2.15 muestra los módulos internos de las PBX: dos tarjetas para interconexión, una en cada PBX, y una tarjeta DISA. Las dos PBX trabajan como una sola gracias a un cable multipar que enlaza las dos tarjetas de interconexión.

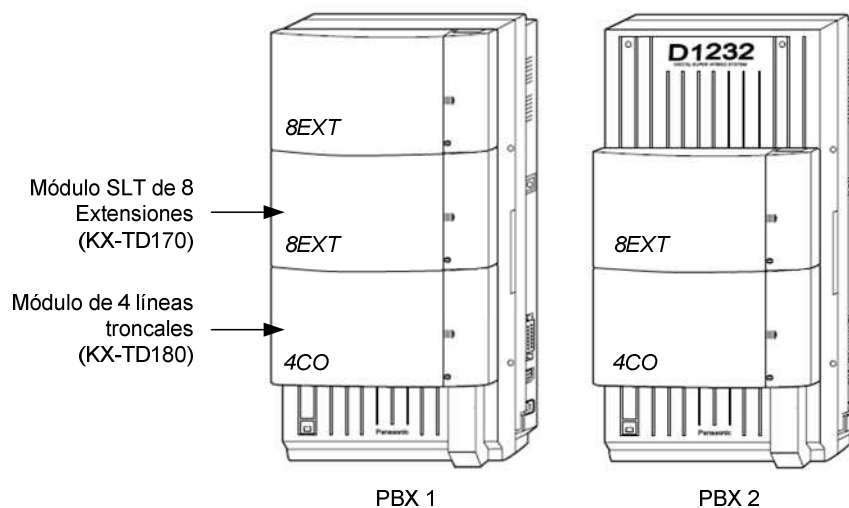


Figura 2.14 *PBX's Panasonic KX-TD1232 de Alianza de Seguros con sus respectivos módulos de extensiones y líneas troncales*

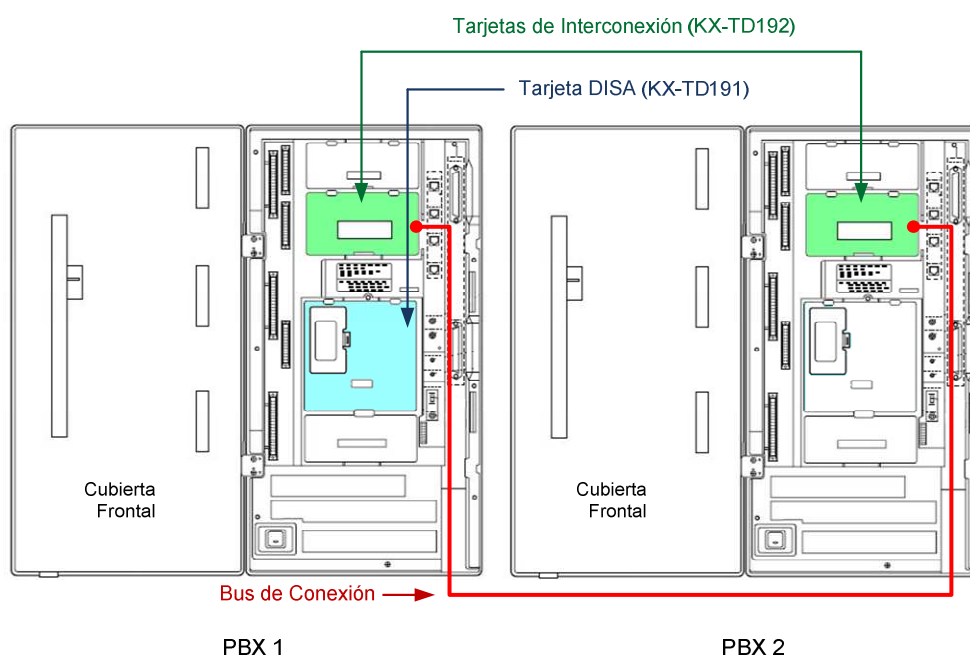


Figura 2.15 *PBX's Panasonic KX-TD1232 de Alianza de Seguros con sus respectivas tarjetas internas de interconexión y DISA*

El tipo de señalización soportada por la PBX KX-TD es DTMF o DP (*Dial Pulse*) tanto para la señalización que recibe de la PSTN como para la que se usa con extensiones internas. Esta señalización le proporciona la capacidad de aceptar terminales telefónicos analógicos o digitales.

La PBX está controlada por un CPU (*Central Processing Unit*) de 16 bits incorporado en la tarjeta principal de la PBX. Este CPU se encarga del procesamiento digital de las funciones de la PBX, que se programan mediante una interfaz de usuario. Las funciones que se pueden programar incluyen el establecimiento de la fecha y hora, adición de extensiones al sistema telefónico, restricción de llamadas, códigos especiales para llamada, etc.

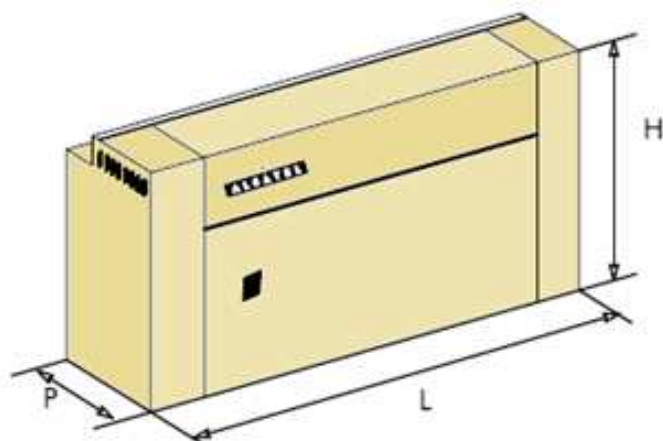
La PBX Panasonic KX-TD1232 permite definir hasta 8 “clases de servicio”, que son niveles de autorización o restricción de llamadas en cada extensión. En Alianza Quito se tienen configuradas 6 clases de servicio, donde el nivel de restricción es mayor mientras más alto es el valor de clase. La clase 1 no tiene ninguna restricción, desde donde se pueden realizar llamadas internacionales o a celular, previa introducción de un código de autorización. Esta clase está asignada a las extensiones de la *Gerencia General*, por citar un ejemplo. La clase 6 permite básicamente la comunicación interna, sin la posibilidad de realizar llamadas salientes a la PSTN. Esta clase está programada para la extensión de la guardianía. Las otras clases varían en su nivel de restricción, siendo las principales limitaciones las llamadas de larga distancia, a celulares y el tiempo de duración de la llamada.

Otra de las funciones programadas en la PBX es la contestadora automática. Todas las llamadas entrantes son atendidas en primera instancia por la contestadora. Si la persona que realiza la llamada conoce la extensión con la que desea comunicarse, puede hacerlo después de escuchar el mensaje de la contestadora, caso contrario la llamada es atendida por la recepcionista.

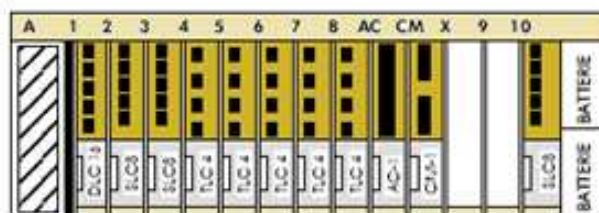
2.1.3.1.2 *Central Telefónica de Guayaquil-centro*^[31]

La sucursal de Guayaquil cuenta con una central telefónica propietaria de marca *Alcatel*. Es una PBX de la serie *Office PRO 4200* modelo M, del tipo modular, con ranuras de expansión para tarjetas adicionales. Esta central admite teléfonos del tipo analógico y digital.

La PBX *Alcatel Office PRO 4200* tiene capacidad máxima para 72 extensiones, 24 troncales analógicas y 32 estaciones portables DECT, mediante módulos para expansión como: teléfonos inalámbricos DECT, hasta 16 canales VoIP IP-LAN, líneas troncales TLC (*Trunk Line Card*), extensiones DLC (*Digital Line Card*) y extensiones SLC (*Single Line Card*).



Central telefónica Office PRO 4200 MODELO M



Slots de la central telefónica y sus tarjetas

Figura 2.16 *PBX Alcatel Office PRO4200* con sus respectivos módulos de extensiones y líneas telefónicas

Esta PBX tiene una capacidad de 10 ranuras de expansión, más una adicional. Se encuentran ocupadas 9 ranuras con tarjetas del tipo: DLC para extensiones digitales, SLC para extensiones analógicas, TLC para la conexión de líneas troncales, AC para el almacenamiento de la música en espera y otras funciones, y MC para el control y tarifación de llamadas. En la tabla 2.23 se muestra la cantidad de tarjetas y sus puertos; en la figura 2.16 se muestra la forma de la PBX Alcatel y la distribución de las tarjetas.

Cantidad	Tarjeta	Puertos por tarjeta	Puertos totales	Puertos Libres	Puertos Usados	TOTAL PUERTOS USADOS
5	TLC (troncales)	4	20	3	17	17 troncales
1	DLC (extensiones digitales)	8x2	16	6	10	27 extensiones
3	SLC (extensiones analógicas)	7	21	4	17	

Tabla 2.23 *Tarjetas ocupadas en la central telefónica y sus puertos*

2.1.3.1.3 Cableado Telefónico

EL cableado telefónico de la matriz en Quito parte del centro del subsuelo del edificio. Bajo el graderío que lleva al subsuelo se encuentra el armario principal que contiene a las dos PBX interconectadas, un cajetín de distribución, la acometida de la PSTN y el respaldo de energía, formado por dos baterías de automóvil de 12 voltios DC.

Todo el cableado telefónico del subsuelo, planta baja y planta independiente se reparte a partir del cajetín de distribución del armario principal, el cual se encuentra conectado a un cajetín de distribución secundario ubicado en el primero piso. Aquí converge el cableado telefónico de los pisos primero y segundo.

Desde el edificio principal salen dos extensiones hacia la planta independiente, donde residen las oficinas de Extern Solut.

El medio utilizado para interconectar a los terminales telefónicos con las PBX es cable multipar de 50 pares, tendido a través de mangueras hacia cada una de las oficinas y conectorizando en las regletas de los cajetines de distribución. Desde los cajetines de distribución todos los pares se conectan a los *jacks* de las PBX, ya sean para extensiones o líneas de la acometida.

En Guayaquil se tiene un único sistema de cableado para voz y datos. La parte telefónica se encuentra instalada con cable UTP categoría 5E y sólo uno de los 4 pares del cable es utilizado.

La central telefónica se encuentra ubicada en el Departamento de Sistemas, lugar en el que se tiene el *rack* de comunicaciones con dos *patch-panels* asignados para las líneas troncales y los puntos de voz. La acometida del servicio telefónico se encuentra ubicada en la entrada principal de estas oficinas. Desde allí ingresan las líneas troncales a una regleta de distribución y, mediante cable multipar y tubería, se extienden al *patch-panel* del Departamento de Sistemas para su interconexión con la PBX.

2.1.3.1.4 Terminales Telefónicos ^[29]^[30]

Los terminales telefónicos que soportan las PBX de Alianza son variados. Entre ellos se encuentran teléfonos analógicos, digitales e inalámbricos, consolas de asistente, altavoces, etc. Estos terminales son propietarios, exclusivos para su uso con determinado modelo y marca de PBX.

En Alianza Quito se usan los siguientes terminales: teléfonos analógicos, digitales, consola de asistente (en recepción), faxes y un dispositivo *datafast*.

Los teléfonos analógicos de modelo Panasonic KX-T7000 y KX-T7300 utilizan dos pares del cable multipar. Cuentan con teclas de función para diferentes tareas, por ejemplo, atender diversas llamadas entrantes, que se muestran mediante señales luminosas. Estos teléfonos tienen un *jack* RJ-11 adicional para conectar un segundo teléfono que actúa como otra extensión de la PBX. Este mecanismo ahorra recursos de cableado.

El modelo KX-T7300, con mayor funcionalidad, se encuentra en las oficinas de gerentes y jefes de área; mientras que el modelo 7000 lo utiliza la mayor parte del personal. Ambos modelos incluyen un altavoz incorporado.

En la recepción se cuenta con un teléfono digital especial. Se trata del modelo KX-T7400 que se conecta con la consola KX-T7340; en total utilizan 4 pares de cable multipar. Este teléfono a diferencia de los anteriores, tiene un *display* retro-iluminado de dos filas y control de volumen para el altavoz. La consola permite manejar todas las llamadas entrantes de la PSTN redirigidas a la recepción. Este terminal permite a la recepcionista comunicar avisos, por el altavoz de cada teléfono, al personal.

Dos tipos de terminales telefónicos no forman parte del sistema telefónico interno de Alianza en Quito y Guayaquil: los faxes y el *datafast*. Estos terminales tienen líneas directas conectadas a ellos con números independientes. Son tratados como un mecanismo de envío/recepción de datos por la PSTN, en lugar de transmisión de voz.

El fax se usa regularmente para enviar y recibir documentos que deben ser revisados en ese instante. En este sentido es una alternativa más rápida que el correo electrónico. El *datafast* se utiliza para el registro de las tarjetas de crédito y para emitir los *vouchers*. Este dispositivo consta de un lector magnético y un teclado numérico para ingresar el número de la tarjeta. Los datos son enviados a través de la línea telefónica a una entidad bancaria para el registro y cargo monetario correspondientes.

La tabla 2.24 resume la cantidad de terminales telefónicos de Alianza Quito.

	Terminales analógicos	Terminales digitales	Consola	Fax	Datafast
SB	19	0	0	1	1
PB	13	1	1	2	0
P1	9	0	0	1	0
P2	1	0	0	0	0
Total					49

Tabla 2.24 *Terminales telefónicos en Alianza Quito*

La sucursal de Guayaquil tiene terminales telefónicos del tipo analógico y digital de la marca Alcatel modelo *Premium-Reflexes* 4020. Además, cuenta con terminales de fax y un terminal telefónico inalámbrico. En la tabla 2.25 se detallan los terminales ubicados en esta sucursal.

Tipo de terminal	Ubicación		Total
	Ala 1	Ala 2	
Teléfono Digital	5	3	8
Teléfono Analógico	6	13	19
Fax	2	2	4
Teléfono Inalámbrico	1	0	1

Tabla 2.25 *Terminales telefónicos en Alianza Guayaquil*

2.1.3.1.5 *Interconexión con la PSTN*

Alianza de Seguros hace uso de los servicios de interconexión de la CNT para mantener la comunicación telefónica con otras sucursales, sus clientes y otras empresas. La interconexión en Quito y Guayaquil se la realiza mediante troncales analógicas y el servicio es accedido mediante los números asignados a cada una de las líneas.

Sucursal	Troncales		Líneas Directas
	PBX	Salida	
Quito	10	12	5
Guayaquil	12	5	5

Tabla 2.26 *Resumen de líneas telefónicas de Quito y Guayaquil*

Si bien la CNT cuenta con infraestructura digital para brindar sus servicios de telecomunicaciones, gran parte del acceso de última milla sigue siendo analógico. Alianza de Seguros, tanto en Quito como Guayaquil, tiene líneas analógicas contratadas con la CNT. Las líneas públicas llegan hasta la acometida con cable multipar. De este grupo de líneas unas van a las PBXs y otras se usan como

líneas directas para faxes y los *datafast*. La tabla 2.26 muestra el número total de líneas telefónicas en Quito y Guayaquil.

En su mayoría, las líneas que Alianza emplea, son para que sus clientes tengan fácil acceso a sus servicios y puedan resolver sus inquietudes. Para ello se ha contratado con la CNT el servicio de líneas PBX. Con este servicio, se utiliza un grupo de las líneas contratadas, para evitar que llamadas entrantes se pierdan. Cada línea PBX tiene su propio número al igual que el resto, pero se tiene un número telefónico primario o de arranque, el cual se desea que el público conozca. Cuando una persona llama a uno de estos números, y se encuentra ocupado, inmediatamente se busca qué línea del grupo está libre para no perder la llamada. Este proceso lo realiza la PSTN transparentemente, sin necesidad de que el usuario vuelva a marcar o utilice un número distinto.

Las demás líneas que no forman parte del servicio PBX de la CNT se usan principalmente para llamadas salientes.

2.1.3.2 Análisis de Tráfico de Voz ^{[3][4][51]}

En el análisis del tráfico de voz se consideró el uso de encuestas a los usuarios (ver modelo de la encuesta en el anexo D) e información proporcionada por la empresa de telecomunicaciones CNT. No se contó con el acceso a la monitorización propia de las centralitas telefónicas.

Las planillas telefónicas o facturas telefónicas de las líneas de Quito y Guayaquil proporcionaron información de la cantidad de llamadas que se realizan diariamente, estimada en base al costo por minuto de la llamada de categoría comercial y la duración promedio de las llamadas. Por medio de las encuestas se pudo determinar en Quito el rango de duración de una llamada de 2 a 5 minutos, con un promedio de 220 segundos. Para la sucursal de Guayaquil se tiene una duración promedio de llamada de 3 a 5 minutos, 240 segundos en promedio. Con estos valores se estimó que la cantidad de llamadas mensuales para Quito y

Guayaquil son 3075 y 4354 llamadas respectivamente. El análisis de tráfico de voz en detalle se encuentra en el anexo E.

Para establecer la cantidad de llamadas diarias se asumió que en el mes existen 20 días laborales, trabajados de lunes a viernes. Así se obtuvo: 154 llamadas diarias para Quito y 218 para Guayaquil. Las encuestas a los usuarios ayudaron a identificar las llamadas internas y externas (hacia la PSTN) de la empresa. Las preguntas se relacionaron con los intentos de llamada que se hacen en un día a: usuarios internos, usuarios de otras sucursales y clientes de la empresa (llamadas hacia la PSTN). Esta información se detalla en porcentajes en la tabla 2.27, donde se observa que la mayor cantidad de llamadas generadas son a clientes de Seguros Alianza tanto en Quito como en Guayaquil.

QUITO		
	# Llamadas diarias	Porcentaje de llamadas
A clientes Alianza	117	76%
A sucursales	14	9%
A Alianza Guayaquil	23	15%
TOTAL	154	100%
GUAYAQUIL		
	# Llamadas diarias	Porcentaje de llamadas
A clientes Alianza	144	66%
A sucursales	30	14%
A matriz Quito	44	20%
TOTAL	218	100%

Tabla 2.27 *Tipo de llamadas y su distribución diaria*

El análisis anterior permite observar únicamente la cantidad de llamadas que se realizan desde Alianza pero no información sobre la hora pico ni el tráfico que se soporta. Para realizar este nuevo análisis se estimó la distribución horaria de las llamadas realizadas. Haciendo uso de las encuestas se distribuyó el horario laboral de la empresa, 8h30 a 17h30, en tres horarios: 8h30-11h30, 11h30-13h30 y 14h30-17h30; de esta manera se puede obtener el porcentaje de llamadas llevadas a cabo en cada rango. En la tabla 2.28 se muestra un resumen de la

estimación del número de llamadas que se realiza diariamente y su respectiva distribución horaria.

QUITO				
	8h30-11h30	11h30-13h30	14h30-17h30	Total
Porcentaje de llamadas	37%	27%	36%	100%
Cantidad de llamadas	57	42	55	154
GUAYAQUIL				
	8:30-11:30	11:30-13:30	14:30-17:30	Total
Porcentaje de llamadas	33%	30%	37%	100%
Cantidad de llamadas	72	66	80	218

Tabla 2.28 *Porcentaje de llamadas y su distribución horaria*

En base a los cálculos anteriores se puede estimar la intensidad de tráfico aproximada que soporta el sistema telefónico. La intensidad de tráfico tiene como unidad el *Erlang* que equivale a una llamada de una hora de duración, considerada en una hora de referencia. Se calcula de la siguiente manera:

$$Vt = n * d$$

Vt: Volumen de tráfico

n: número de llamadas

d: duración promedio de cada llamada

$$It = \frac{Vt}{T}$$

It: Intensidad de tráfico

T: Periodo de tiempo de observación o referencial

En la tabla 2.29 se muestra el volumen y la intensidad de tráfico para el rango de horas mostradas en la tabla 2.28.

De lo mostrado en la tabla 2.29 se puede observar que el horario de mayor intensidad de tráfico es desde las 11h30 hasta las 13h30, es decir las horas pico. En este horario se realiza la mayor cantidad de llamadas, sean éstas hacia las sucursales o clientes de la empresa. Además, se puede identificar que el tráfico generado por la sucursal de Guayaquil es mayor que el de la matriz de Quito, debido en gran medida a la cantidad de llamadas que se realizan de Guayaquil a Quito.

Quito				
Duración promedio de llamada [seg]	220			
	8:30-11:30	11:30-13:30	14:30-17:30	Total Diario
Cantidad de llamadas	57	42	55	154
Volumen de tráfico[seg]	12514,17	9131,96	12175,95	33822,09
Tiempo de referencia [horas]	3	2	3	8
Intensidad de tráfico [Erlangs]	1,16	1,27	1,13	1,17
GUAYAQUIL				
Duración promedio de llamada [seg]	240			
	8:30-11:30	11:30-13:30	14:30-17:30	Total Diario
Cantidad de llamadas	72	66	80	218
Volumen de tráfico [seg]	17280,00	15807,50	19286,37	52373,88
Tiempo de referencia [horas]	3	2	3	8
Intensidad de tráfico [Erlang]	1,60	2,20	1,79	1,82

Tabla 2.29 *Volumen e Intensidad de tráfico telefónico*

2.2 RESULTADOS DEL ANÁLISIS DE LA SITUACIÓN ACTUAL

Luego de haber analizado los elementos pasivos y activos de la red corporativa, incluidos los servicios y su funcionamiento, se procederá a hacer una evaluación global de la red enfocada en los siguientes aspectos:

- Rendimiento
- Escalabilidad
- Disponibilidad
- Administración

- Calidad de Servicio, y
- Seguridad

2.2.1 RENDIMIENTO

Los elementos de la red de datos con mayor carga son los servidores, seguidos de los equipos de conectividad y por último, los terminales. Sin embargo, el porcentaje de utilización de estos elementos en el peor de los casos no llega a superar el 50%, ya sea en procesador, memoria, almacenamiento o uso ancho de banda. A simple vista se podría argumentar que estos elementos soportan una mayor carga sin inconvenientes. No obstante, esta aparente abundancia de recursos se debe a un sobredimensionamiento inicial. Por ejemplo, los servidores cuentan con procesadores de 4 núcleos, de los cuales apenas se utiliza un 25% de su capacidad nominal. Un escenario similar se presenta entre los dispositivos terminales, en cuanto a memoria y almacenamiento. Se necesita la reorganización de estos equipos.

En el caso de los equipos de conectividad, el principal *switch* que sostiene la red LAN de Quito es el 3COM 4200. A pesar de ser un equipo robusto, en algunas ocasiones ha presentado caídas, sobre todo por no estar optimizado para trabajar como núcleo de la red. Adicionalmente, existen *switches* con puertos de acceso *Giga Ethernet*, pero al carecer de capacidades administrativas, tienen un bajo rendimiento.

El sistema telefónico se encuentra en estado crítico. Tanto en Quito como en Guayaquil, las centralitas telefónicas y el cableado han agotado la posibilidad de expansiones y actualizaciones, por lo que se encuentran operando al máximo de sus capacidades. Por esta razón es necesario su pronto reemplazo.

Por otra parte, se ha visto que la tecnología *Fast Ethernet* de 100 Mbps, en la cual se basa la red LAN, es suficiente para soportar el tráfico de todos sus servicios. El ancho de banda máximo utilizado en los enlaces más congestionados, es decir,

de los servidores, no supera los 17 Mbps (ver tabla 2.22). Así se concluye que las NIC *Giga Ethernet* presentes en algunos servidores están subutilizadas.

Del enlace WAN de Quito, por donde pasa todo el tráfico de las sucursales, se utiliza como máximo el 60% de su capacidad total (fig. 2.19). Aunque este grado de utilización parece elevado, se debe aclarar que, incluso considerando un margen de seguridad del 20%, existe un 20% restante que está sobredimensionado. Esto es importante ya que esa capacidad desperdiciada implica un costo innecesario que la empresa afronta mensualmente.

2.2.2 ESCALABILIDAD

Los principales problemas de escalabilidad encontrados en la red corporativa de Alianza tienen que ver con el cableado y los equipos de conectividad.

El cableado en las redes de Quito y Guayaquil tiene suficientes puntos para el crecimiento previsto. Sin embargo, en la red de Quito el cableado no está basado en estándares, por lo que esos puntos de red no son confiables. Adicionalmente, no es posible añadir nuevos equipos debido a que todos los *switches* y servidores se almacenan actualmente en un único cuarto, el cual no cuenta con mayor espacio para expansión.

Los equipos de conectividad no cumplen sus funciones en base a un modelo de planificación organizado, como el modelo jerárquico. Si se requiere añadir una estación de trabajo y no se encuentran puertos disponibles en los *switches* de acceso, es común utilizar los puertos libres del *switch* que funge de núcleo, o a su vez recurrir a *switches* de baja calidad, no planificados, para suplir esta necesidad. Cuando estos equipos cumplen funciones no previstas se complica el esquema de red y es muy difícil que sea escalable. Por esta razón es necesario descartar los *switches* no planificados y reubicar a los otros dependiendo de sus capacidades, en un modelo organizado.

Los servidores de base de datos o antivirus soportan más usuarios que los existentes en Alianza, alrededor de 90, por lo que no suponen un problema de crecimiento. Para los servicios restantes es necesario su reordenamiento y en el caso particular del servicio de correo, éste debe ser separado del equipo que brinda las funciones de *firewall*.

2.2.3 DISPONIBILIDAD

Entre las principales razones por las que los servicios de red presentan *downtimes* se cuentan las fallas en la energía eléctrica, caída del enlace de datos e Internet, modificación de configuraciones, y manipulaciones o daños accidentales de los servicios y equipos de la red.

Aunque la matriz en Quito cuenta con un generador eléctrico a diesel para casos de emergencias eléctricas, el tiempo que éste se demora en dar energía al edificio es de aproximadamente 10 minutos. El UPS (*Uninterruptible Power Supply*) sólo tiene respaldo suficiente para mantener activos a los servidores y *switches* principales durante el cambio al generador, por lo que si se agregan equipos extras es necesario aumentar su capacidad.

La caída del enlace de datos e Internet es esporádica y variable, acumulándose en una jornada laboral hasta media hora de *downtime*. Dado que la mayor parte de servicios se brindan desde Quito a través del enlace WAN, se debe aumentar la disponibilidad de este enlace.

Cuando se trata de modificar las configuraciones, añadir características a los servicios existentes o sencillamente dar mantenimiento, en algunas ocasiones se deja sin servicio a los usuarios. Esta falencia puede ser reducida o descartada con la debida planificación para este tipo de eventos.

Por otro lado, las manipulaciones indebidas y los daños accidentales se producen principalmente porque los equipos de red y el cableado están expuestos a usuarios no autorizados, o a que las medidas de seguridad fallan. Una posible

solución a esta problemática es establecer políticas para el manejo de la información y recursos de red más la implantación de mecanismos de seguridad confiables.

2.2.4 ADMINISTRACIÓN

La empresa cuenta con algunos lineamientos para la administración de la red corporativa, como los acuerdos de nivel de servicio con el proveedor WAN o la utilización de productos *Microsoft* como plataforma de *software* en las estaciones de trabajo, pero estos lineamientos son insuficientes.

Actualmente se cuenta con una gama muy variada de *switches*, servidores, computadores y también de *software*. La mayoría de *switches* son de marcas heterogéneas y carecen de cualquier función de administración. Entre servidores, computadores de escritorio y laptops se encuentran diferentes familias de procesadores (*Power5*, *AMD* e *Intel*). Entre los sistemas operativos, se tienen plataformas propietarias como el AIX de IBM o *Windows XP* de *Microsoft*, y libres como *Linux*. Esta heterogeneidad complica el modelo administrativo.

En general, la red carece de estándares y normas para la implementación y la gestión de la tecnología. El principal problema se evidencia con el manejo de la infraestructura, sobre todo el cableado en Quito que no cumple las normas ANSI/EIA/TIA.

Otro inconveniente es el seguimiento y control de los activos locales y remotos de la red. No se ha implementado una herramienta robusta de gestión y administración para los equipos ni para el personal de la empresa, que permita llevar el registro y estadísticas sobre el estado actual de los servicios y el funcionamiento de los diversos equipos. La heterogeneidad de los componentes y la distribución geográfica de la red exigen una herramienta de administración centralizada y estandarizada que a través de su información permita la toma de decisiones y resolución de fallos.

2.2.5 CALIDAD DE SERVICIO ^[5]

La red corporativa no está lista para brindar calidad de servicio a las aplicaciones en tiempo real. En primer lugar, el cableado en Quito tiene varias falencias como se ha descrito en los ítems anteriores. En segundo lugar, la red no está apta para brindar priorización de tráfico a los paquetes. La mayoría de *switches* tanto en Quito como Guayaquil no soportan VLANs (IEEE 802.1q) ni diferenciación de servicios (802.1p).

El excedente de ancho de banda en las LAN o la WAN no garantiza por sí solo que los paquetes de voz tengan preferencia sobre los paquetes de datos en caso de saturación. Por otro lado, se deben ajustar los parámetros de disponibilidad, retardos y *jitter* del enlace WAN en el SLA existente entre Alianza y el *carrier*.

2.2.6 SEGURIDAD

En varios aspectos, la red de Alianza de Seguros y su información están expuestas a diversas amenazas internas y externas. Dentro de las amenazas internas se tiene que los servidores y equipos críticos de conectividad están expuestos a personal no autorizado, lo que puede incurrir en daño o robo de equipos, con la consecuente falla en los servicios.

La mayoría del tráfico atraviesa la red en texto plano, lo que facilita el robo de información mediante herramientas de *sniffing*. Esto es factible pues se pueden incrustar *hubs*, *access points* o laptops no autorizados en la red, ya que no se autentica a los dispositivos terminales. Los perfiles de usuario, administrados a través de *Active Directory*, sólo controlan el acceso a los recursos de computadores y servidores basados en el sistema operativo *Microsoft Windows*, por lo que los recursos de otras plataformas requieren mecanismos de autenticación diferentes. El *firewall/proxy* controla en cierta medida las amenazas externas mediante restricciones. Aún así, existen virus informáticos y troyanos

que se cuelan a través de Internet o de memorias USB, así como *spyware* que se aloja en el correo electrónico, incluso en presencia del *software* antivirus

2.3 ANÁLISIS DE REQUERIMIENTOS ^{[1][32]}

Del apartado anterior se concluye que se requiere el rediseño de la red corporativa, no sólo para optimizar el funcionamiento de los servicios existentes, sino también para añadir otros. A continuación se definen los requerimientos para el rediseño de las redes LAN de Quito y Guayaquil, para la integración de la red de voz y datos, y para el redimensionamiento del enlace WAN y acceso a la PSTN. Las proyecciones y el crecimiento se estimarán para un lapso de 5 años.

2.3.1 REQUERIMIENTOS PARA LAS REDES LAN DE QUITO Y GUAYAQUIL

A continuación se definen los requerimientos para la parte pasiva y activa de las redes locales de Quito y Guayaquil.

2.3.1.1 Infraestructura de cableado estructurado

De acuerdo al análisis realizado de la situación actual de la red, se concluye que para la ciudad de Quito se debe realizar un nuevo diseño de cableado estructurado, ya que el sistema actual carece de las prestaciones necesarias y ha cumplido ya su tiempo de vida útil. Para Guayaquil se mantendrá el mismo sistema de cableado estructurado, ya que tiene menos de 3 años de funcionamiento, y que cumple con las normas y estándares ANSI/EIA-TIA así como con las pruebas de certificación realizadas. Para este sistema se requiere únicamente realizar algunas recomendaciones para su administración.

Para la nueva infraestructura de cableado estructurado en Quito y la actual de Guayaquil se requiere:

- Facilidad en la gestión y administración del sistema de cableado estructurado. En Guayaquil se requiere únicamente la correcta etiquetación para llevar la documentación completa del sistema.
- Segmentar las redes de voz y datos utilizando diferente tipo de color de cable en los *racks* respectivos.
- Reorganizar los cuartos de equipos y telecomunicaciones.
- Utilizar el cableado adecuado, sin mezclar categorías. Para la elección de la categoría se considerará el ancho de banda que cursará por la red.
- Cumplir con las normas ANSI/EIA-TIA de cableado estructurado en el diseño del nuevo sistema de cableado y mantener su cumplimiento en el sistema ya establecido de Guayaquil.
- Mejorar la seguridad física y acceso hacia los cuartos de equipos y telecomunicaciones, para evitar la irrupción por parte de personal no autorizado.
- Mejorar las condiciones de climatización dentro de los cuartos de equipos y telecomunicaciones para evitar el sobrecalentamiento de los equipos o posibles fallas en los componentes eléctricos y electrónicos debido a la humedad.

2.3.1.2 Estructura de la red LAN

Para la nueva estructura de la red LAN se requiere:

- Sencilla escalabilidad de equipos activos. La nueva estructura deberá facilitar la adición o crecimiento de usuarios de la red y la adición de nuevas tecnologías y servicios.
- Incrementar la disponibilidad, ya que se añadirá al *pool* de servicios de red ofrecidos, el servicio de Telefonía IP. El uso de la tecnología PoE para teléfonos será considerado dentro del diseño.
- Características de seguridad en los equipos activos, importantes para evitar ataques internos y consecuentemente la pérdida, tergiversación y mala utilización de la información.

- Características de administración y gestión en los equipos activos de la red, de tal manera que se puedan monitorear y detectar a tiempo posibles inconvenientes para tomar los correctivos respectivos.
- Mantener los servicios de red actuales más los servicios de voz y gestión. Para el monitoreo de la red se considerará el protocolo SNMP.
- Redimensionar los servidores que se consideren subutilizados y en caso de que un servidor se encuentre saturado, se balanceará la carga del mismo.
- Determinar las características mínimas necesarias para los equipos de red, y escoger los equipos actuales que se puedan reutilizar.
- Características de calidad de servicio adecuadas para priorizar el tráfico en la red convergente de voz y datos.
- Dimensionar las aplicaciones que soportará la central telefónica IP, así como las características mínimas a soportar para su funcionamiento.
- Definir políticas básicas de administración y seguridad.

2.3.2 REQUERIMIENTOS PARA LA INTEGRACIÓN DE VOZ Y DATOS

El servicio de Telefonía pasará a formar parte de la red de datos, para lo cual se presentan tres niveles de integración disponibles:

- **Voz sobre IP.** En este nivel de integración sólo el tráfico de voz pasa a formar parte de la red IP. No se consideran servicios adicionales.
- **Telefonía IP.** Además del tráfico de voz, se consideran servicios adicionales como la administración y registro de llamadas, presencia, fax y mensajería instantánea, videoconferencia, etc., integrados con servicios existentes como el correo o las bases de datos.
- **Comunicaciones Unificadas.** Éste se considera el nivel de integración más avanzado. Abarca los servicios existentes de la red, Telefonía IP, video y tecnologías multimedia en general, para integrarlos bajo un esquema de productos y servicios de múltiples proveedores.

Dada la infraestructura y los servicios con los que opera Alianza de Seguros, el nivel de integración más adecuado para este proyecto es el de Telefonía IP, con el que se posibilita una posible migración hacia comunicaciones unificadas.

2.3.2.1 Funciones del Sistema de Telefonía IP

Entre las funciones más importantes del sistema de Telefonía IP se requerirá:

- Fax, mensajería instantánea y buzón de voz, integrados con el servicio de correo electrónico mediante protocolos IMAP, POP3 y SMTP.
- Servicio de presencia, donde se pueda indicar el estado de disponibilidad del usuario.
- Integración con el servicio de directorio a través del protocolo LDAP.
- Integración con el servicio de bases de datos DB-2 de IBM.
- La administración de permisos y bloqueos de llamadas en función a un perfil de usuario.
- Acceso seguro a información del usuario y encriptación de los canales de voz.
- Una herramienta de gestión centralizada de acceso fácil y seguro desde la cual se puedan administrar las cuentas de usuarios y hacer el seguimiento de las llamadas mediante un registro de forma local o remota.
- El soporte de conferencias de voz, donde usuarios de las dos sucursales puedan iniciar, unirse o abandonar una conferencia.
- Terminales telefónicos con funciones varias tales como: parqueo, transferencia, levantamiento, reenvío e historial de llamadas, llamada en espera, música en espera, etc.
- Funciones de contestadora automática.
- La posibilidad de que el sistema telefónico se expanda con funciones avanzadas como el reconocimiento de voz, *text-to-speech*, IVR (*Interactive Voice Response*) o ampliación a *call center*.
- Interacción con la PSTN y redes de ISP.

Adicionalmente, se requiere definir los códecs de voz que se utilizarán para el tráfico de voz.

2.3.2.2 Análisis y Elección de Códecs ^{[2][3][34]-[48]}

Para seleccionar los códecs de voz más adecuados para este proyecto se procederá a analizar los factores que afectan la calidad de audio y la complejidad que presentan para su implementación.

Dos factores afectan directamente la calidad sonora que producen los códecs y el ancho de banda que requieren, los cuales son: el rango de frecuencias que admite el codificador y el método de compresión utilizado.

Antes de digitalizar la voz se filtra el rango de frecuencias que ingresa al codificador para eliminar componentes innecesarias y así disminuir el ancho de banda requerido. En la Telefonía tradicional, las frecuencias admitidas están entre 300 Hz y 3.4 kHz, considerándose que en este rango la voz es completamente inteligible. A los códecs que trabajan dentro de este rango se los clasifica como códecs de banda estrecha (*Narrow Band*, NB) y utilizan una frecuencia de muestreo de 8 kHz. No obstante, para aumentar la fidelidad auditiva, existen códecs que admiten un rango de frecuencias mayor, entre 50 Hz y 7 kHz (Fig. 2.17). Estos códecs se denominan de banda ancha (*Wide Band*, WB) y operan con una frecuencia de muestreo de 16 kHz.

Como segundo factor, el método de compresión es el responsable de que la señal de voz sea reconstruida con mayor o menor precisión. El método más simple de compresión es PCM (*Pulse Code Modulation*); con la mayor velocidad de codificación, 64 kbps, no es la técnica más eficiente. Su principal deficiencia es que no toma en cuenta las pequeñas variaciones de las señales de voz. Así aparece un avance, ADPCM (*Adaptive Differential PCM*); esta técnica aprovecha la gran similitud entre las muestras de voz adyacentes, calcula la diferencia y la codifica con un número de bits menor y adaptable. Con ADPCM se puede reducir la velocidad de codificación necesaria a la mitad, 32 kbps.



Figura 2.17 Rangos de frecuencia de banda estrecha y banda ancha

Otro método para reducir aún más el ancho de banda requerido por el códec, es CELP (*Code Excited Linear Predictive*). Este método, más complejo, consiste en transmitir la información mínima necesaria para reconstruir la señal de voz a través de un modelo predictivo lineal del tracto vocal. Con CELP se consiguen velocidades de codificación en el orden de los 8 kbps. Alrededor de las técnicas descritas, existen variantes que mejoran la calidad auditiva y/o reducen el consumo de ancho de banda. Una lista de los códecs más utilizados se muestra en la tabla 2.30.

Códec Estándar	Método de Compresión	Tipo de Banda	Frecuencia Muestreo [kHz]	Bit Rate [kbps]	Payload de Voz ¹ [ms]	Payload de Voz [byte]	MOS ²
G.711	PCM	NB ³	8	64	20	160	4.1
G.723.1	MPMLQ	NB	8	6.3	30	24	3.9
G.723.1	ACELP	NB	8	5.3	30	20	3.8
G.726	ADPCM	NB	8	32	20	80	3.85
G.728	LDCELP	NB	8	16	30	60	3.61
G.729	CS-ACELP	NB	8	8	20	20	3.92
G.729a	CS-ACELP	NB	8	8	20	20	3.9
GSM FR	RPE-LTP	NB	8	13	20	33	3.3/3.4
G.722	SB-ADPCM	WB ⁴	16	64	20	160	4.2
G.729.1	CELP, TDBWE, TDAC	WB	16	32	20	80	4.4

¹ Tamaño típico del payload de voz en milisegundos

² La lista incluye únicamente el MOS para la máxima velocidad de codificación de cada códec

³ NB: *Narrow Band*, banda estrecha

⁴ WB: *Wide Band*, banda ancha

Tabla 2.30 Códecs de audio para Telefonía IP

a columna 1 indica los códecs estandarizados. Los códecs de la serie G.7xx son estandarizados por la ITU-U y el códec GSM (*Global System for Global Communications Full-Rate*) es estandarizado por la ETSI (*European Telecommunications Standards Institute*). De las columnas 2 a la 7 se muestran las características propias de cada códec, desde el método de compresión utilizado, hasta el tamaño típico de la trama de voz. La columna 8 muestra el MOS (*Mean Opinion Score*) que se refiere a la calidad auditiva percibida. La calidad máxima en esta escala se representa con el valor 5. Como se puede ver, los códecs con la mejor calidad en orden descendente son G.729.1 y G.722, de banda ancha, seguidos por G.711 y G.729, de banda estrecha.

Aparentemente, el códec G.729.1 es la mejor opción dado su alto MOS y su bajo ancho de banda requerido (32 kbps). Sin embargo, el algoritmo de este códec es muy complejo y requiere chips DSP (*Digital Signal Processor*) muy potentes; adicionalmente, ha sido recientemente estandarizado y son pocos los equipos que lo soportan. Estas características hacen que esta opción sea costosa actualmente, aunque próximamente se convertirá en una alternativa viable.

Los códecs G.711 y G.722 trabajan con el mismo ancho de banda, 64 kbps, y tienen un MOS similar. El primero es el más simple de todos, por lo que requiere pocos recursos computacionales. Gracias a esto, es el códec más ampliamente difundido en equipos de Telefonía y es una buena alternativa para tráfico interno de la red LAN. El segundo se está difundiendo con celeridad en Telefonía con audio de alta definición, por ser de banda ancha. En comparación con el códec G.729.1, requiere menos ciclos del procesador para la codificación/decodificación, por lo que es una opción válida para aumentar la fidelidad del audio en la LAN. Se propondrá el uso de los códecs G.711 y G.722 para el tráfico interno de las sucursales, con preferencia en el primero, por su compatibilidad con la mayoría de productos existentes.

Para finalizar, el códec G.729, con un MOS de 3.92 y una velocidad de codificación de 8 kbps, es la alternativa más recomendable para el enlace WAN, donde el ancho de banda es escaso.

2.3.3 REQUERIMIENTOS PARA EL ENLACE WAN Y CONEXIÓN CON LA PSTN ^[50]

El principal requerimiento para el enlace WAN y para el acceso a la PSTN es conocer qué cantidad de tráfico soportarán. En este caso se calculará el número de llamadas simultáneas que deberán transportarse por el enlace WAN y el número de circuitos que se necesitarán para acceder a los servicios de la PSTN.

2.3.3.1 Llamadas Simultáneas entre Sucursales

Para el cálculo de las llamadas simultáneas se utilizará la cantidad de llamadas que se realizan entre Quito y Guayaquil en la hora pico, obtenidas del análisis del tráfico de voz. Se consideró que la duración de una llamada promedio es de 240 segundos. Al igual que para el cálculo de circuitos recomendados para la conexión hacia la PSTN, se utilizó la herramienta de cálculo interactiva *online* de *Erlang B*; con una probabilidad de bloqueo del 1% para asegurar que las llamadas entre empleados se puedan realizar sin dificultades. En la tabla 2.31 se muestran los valores resumidos del tráfico proyectado y de los circuitos recomendados.

		Cantidad
Llamadas entre sucursales*		18
Duración de llamada [seg]		240
Intensidad de tráfico [Erlang]	Actual	0.6
	Proyectado	0.7
Circuitos recomendados		4

* Se obtiene de la suma de los valores de llamadas a Guayaquil y llamadas a Quito de las tablas E.11 y E.14 del anexo E.

Tabla 2.31 *Tráfico proyectado y circuitos recomendados*

Para tener una adecuada calidad de llamadas generadas entre sucursales es necesario asegurar un canal con un ancho de banda que soporte los 4 circuitos recomendados en el enlace WAN Quito- Guayaquil.

2.3.3.2 Tipo y número de circuitos troncales hacia la PSTN

Los circuitos troncales hacia la PSTN se calculan usando la fórmula de *Erlang B*. Para ello se tomó la intensidad de tráfico de voz del análisis de la hora pico (tabla 2.29); descartándose el tráfico entre Quito y Guayaquil que cursará por el enlace WAN de la red corporativa de Seguros Alianza.

Con las consideraciones planteadas se procederá a proyectar el tráfico de voz aproximado que se tendrá en 5 años. El tráfico proyectado se obtiene mediante una regla de tres simple en base a las extensiones que se prevé tener en el tiempo indicado. En la tabla 2.32 se resume el tráfico proyectado en 5 años y la cantidad de circuitos de salida recomendados, en base a la cantidad de llamadas de la PSTN en la hora pico. Mediante una herramienta interactiva *online* se realizó el cálculo de *Erlang B* con una la probabilidad de bloqueo 1%, obteniéndose como resultado 5 circuitos mínimos de salida para Quito y 7 para Guayaquil.

		Quito	Guayaquil
Llamadas PSTN proyectadas en hora pico *		37	55
Duración de llamada [seg]		220	240
Intensidad de tráfico [Erlang]	Actual	1,1	1,8
	Proyectado	1,3	2,1
Circuitos mínimos de salida		5	7

* Se obtiene al sumar las llamadas a clientes y a otras sucursales de las tablas E.11 y E.14 del anexo E

Tabla 2.32 *Proyección de tráfico en 5 años*

Por datos proporcionados por el Departamento de Recursos Humanos, la empresa recibe aproximadamente el doble de las llamadas que realiza, dado el número de clientes que tiene y que se encuentran en constante comunicación con la empresa por motivo de los seguros contratados. Por esta razón se asume que el tráfico que soportará la central IP como entrada, producto de las llamadas que hacen los clientes hacia Alianza a través de la PSTN, será el doble del tráfico proyectado para la salida. Tomando en cuenta esta directiva, se encontró que el actual número de troncales de entrada, cumple con estos valores aproximadamente, por lo que se mantendrá el mismo número de troncales de

salida actual, es decir 10 para Quito y 12 para Guayaquil. En total la conexión con la PSTN contará con 15 troncales para Quito y 19 para Guayaquil.

Para mantener el esquema de comunicación con los clientes de Alianza, se conservarán las actuales líneas de fax pero se conectarán directamente con la central de Telefonía IP, como parte del esquema de mensajería unificada. En la tabla 2.33 se muestra en resumen las líneas troncales de entrada y salida necesarias en centralita IP, así como las líneas de fax y *datafast* a utilizarse.

Líneas troncales	QUITO	GUAYAQUIL
Entrada PBX	10	12
Salida	5	7
Fax	4	4
Datafast (voucher)	1	1

Tabla 2.33 *Resumen de líneas troncales a utilizarse*

2.3.4 CRECIMIENTO DE USUARIOS

Alianza de Seguros es una empresa que ha ido variando su personal a lo largo de sus más de 20 años de existencia. La tendencia ha sido incrementar el número de empleados, a medida que se han creado nuevos departamentos y se han abierto nuevas sucursales. Sin embargo, este crecimiento es paulatino. Esto se debe a que, cuando aumentan departamentos y sucursales, se lo hace reasignando al personal existente, con pocas contrataciones nuevas, o fusionando departamentos. Según el Departamento de Recursos Humanos, en los próximos 5 años se espera tener un crecimiento de personal del 10% aproximadamente. Esta proporción es común entre todas las sucursales y será utilizada como base para las estimaciones del crecimiento en Quito y Guayaquil. En la tabla 2.34 se presenta el número de empleados al que se espera llegar en los próximos 5 años, tanto para Quito como para Guayaquil.

Además del número de empleados, según datos proporcionados por la empresa, se esperaría abrir dos sucursales más en el periodo previsto.

Sucursal	Empleados		
	Año 2010	10%+	Año 2015
Quito	57	6	63
Guayaquil	32	4	36

Tabla 2.34 *Crecimiento estimado del personal de Alianza en 5 años*

2.3.4.1 Proyección de usuarios de datos

En Alianza de Seguros no todo el personal hace uso de la red de datos; dependiendo de su actividad y del departamento al que pertenecen hacen o no uso de los diferentes servicios informáticos de la compañía. El personal administrativo y de operaciones cuenta con acceso bajo autenticación a estos servicios, mientras que el personal de mantenimiento y servicios generales no tiene ningún tipo de acceso. Debido a las condiciones expuestas, el número de empleados de la empresa no es idéntico al número de usuarios de la red de datos.

Como dispositivos terminales de la red de datos se encuentran los computadores personales de los usuarios y las impresoras de red; todos ellos conectados a la red cableada. En la tabla 2.35 se resume el crecimiento de los puntos de red necesarios para usuarios e impresoras.

Quito			
	Año 2010	10%+	Año 2015
Usuarios de Datos	52	6	58
Impresoras	7	1	8
Total Puntos de Datos	59	6	65
Guayaquil			
	Año 2010	10%+	Año 2020
Usuarios de Datos	25	3	28
Impresoras	6	1	7
Total Puntos de Datos	31	4	35

Tabla 2.35 *Crecimiento de usuarios de red de datos*

2.3.4.2 Proyección de usuarios de voz

El sistema telefónico actual no presta servicio a todos los empleados de la empresa debido a que los usuarios actuales del sistema telefónico son determinados por el número de ambientes físicos de trabajo en el que se desenvuelven. Son considerados ambientes físicos de trabajo las oficinas, módulos de trabajo, sala de reuniones, comedor, archivo, *suite* y *guardianía*. No obstante, existen lugares sin extensiones telefónicas por ser poco necesarias o porque hay un acceso cercano al servicio. En la tabla 2.36 se muestra en resumen el número de usuarios para Quito y Guayaquil dependiendo del tipo de empleados especificados en la sección 2.1.1.3.3

QUITO		
Tipo de Empleado	Número de Empleados	Usuarios actuales del sistema telefónico
Administrativo	16	15
Operaciones	37	27
Mantenimiento	4	3
TOTAL	57	45
GUAYAQUIL		
Tipo de Empleado	Número de Empleados	Usuarios actuales del sistema telefónico
Administrativo	10	7
Operaciones	20	20
Mantenimiento	2	0
TOTAL	32	27

Tabla 2.36 *Número y tipo de usuarios de voz para Quito y Guayaquil*

Actualmente el sistema telefónico cuenta con un total de 45 extensiones para la ciudad de Quito y 27 extensiones para la ciudad de Guayaquil, siendo esta distribución menor en relación al número de empleados que se tiene.

En las proyecciones del crecimiento del sistema telefónico se consideran las extensiones de los usuarios y las máquinas de fax, las cuales se ubicarán con puntos de red individuales. La tabla 2.37 muestra el crecimiento en el número de puntos de voz.

Para facilitar el cambio de usuarios entre áreas de trabajo y el incremento de empleados en los distintos departamentos, se considerará que por área de trabajo se tendrán dos puntos de red, uno para datos y otro para voz. Sin embargo, existen lugares específicos donde sólo se necesitará un punto de voz uno de datos exclusivamente, para faxes o impresoras.

Quito			
	Año 2010	10%+	Año 2015
Usuarios de Voz	45	5	50
Fax	5	1	6
Total Puntos de Voz	50	6	56
Guayaquil			
	Año 2010	10%+	Año 2015
Usuarios de Voz	27	3	30
Fax	5	1	6
Total Puntos de Voz	32	4	36

Tabla 2.37 *Crecimiento de usuarios de voz*

2.3.5 PROYECCIONES DEL TRÁFICO DE RED

Luego de determinar el número de usuarios que accederán a los servicios de la red, es necesario estimar el tráfico que se generará. Las estimaciones se harán en base a 3 factores: muestras del tráfico actual de la red, estadísticas sobre los datos transmitidos y estadísticas sobre el uso de la red telefónica.

Para el servicio de Telefonía IP se escogerán los códecs de audio que se usarán tanto en la red LAN como en la WAN y se procederá a estimar el tráfico de voz IP para cada caso.

2.3.5.1 Ancho de banda requerido por servicio

La red corporativa deberá soportar los servicios descritos en la sección 2.1.2.4, servicios y aplicaciones de red, más los nuevos servicios de Telefonía IP y administración de red. Los datos de tráfico a los que se harán referencia, han sido

obtenidos desde un dispositivo cliente en condiciones de red no saturada, para garantizar que las velocidades son las necesarias para cada servicio.

2.3.5.1.1 Base de Datos

El tráfico debido a las consultas al servidor de bases de datos es uno de los más bajos de la red. Según las estadísticas de la tabla 2.38, obtenidas de un computador que accede regularmente a la base de datos, se tiene la siguiente información:

# Transacciones / Hora	Duración Transacción [seg]	Volumen Transacción / In [byte]	Volumen Transacción / Out [byte]	Velocidad In [kbps]	Velocidad Out [kbps]
1906	1.89	2350	455	1.927	9.953

* Los datos de entrada/salida se capturaron en el dispositivo Cliente.

Tabla 2.38 *Estadísticas de las transacciones realizadas por hora entre un cliente y el servidor de la base de datos*

Como se puede apreciar en la tabla 2.38, el número de transacciones por hora es elevado. Sin embargo, estas transacciones no representan una alta carga para la red por dos razones: el volumen de datos en cada transacción no es mayor a 3 KB y el tiempo de duración de cada transacción está limitado por la velocidad de respuesta del usuario. En cada transacción se consideran los bytes que el cliente utiliza para realizar una petición y los bytes que el servidor utiliza para responder. Tomando en cuenta los bytes de entrada y salida por cada transacción, se puede estimar que la velocidad de entrada de datos hacia el cliente es de 9.95 kbps y la velocidad de salida es de 1.93 kbps. Estos valores representan las velocidades de entrada y salida necesarias por cada usuario para el acceso a la base de datos.

De las estadísticas tomadas en la semana de mayor tráfico de la red, se tiene que el número máximo de usuarios simultáneos en el servidor de bases de datos actual es de 71 (figura 2.18).

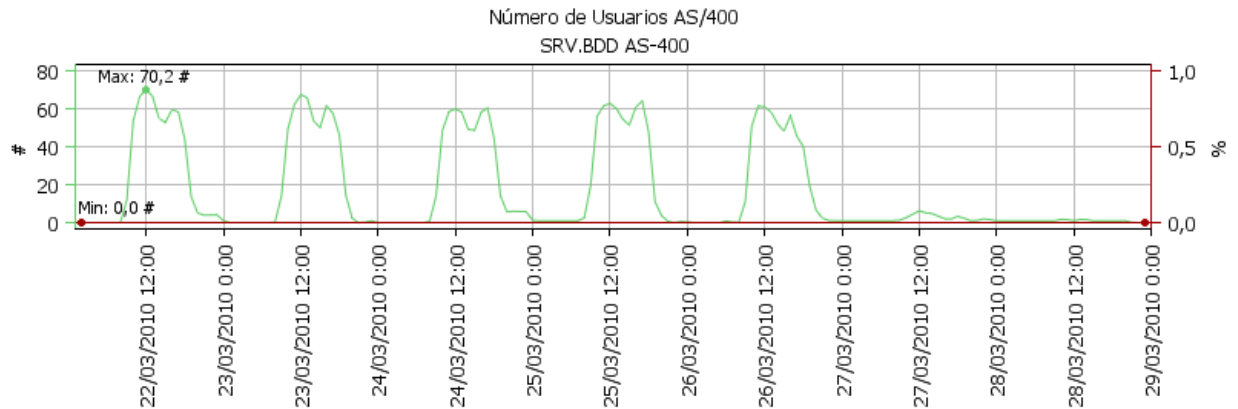


Figura 2.18 Número de usuarios simultáneos del servidor de base de datos.
semana del 22 al 29 de marzo 2010

2.3.5.1.2 Servicio de Aplicaciones

El servicio de aplicaciones, en el que intervienen dos computadores ligeros y el servidor, es altamente interactivo ya que la comunicación entre cliente y servidor se produce durante toda la jornada laboral. Otra característica de este servicio es que el tráfico generado es casi constante. El volumen de datos capturado en el servidor debido a la interacción con un cliente es de 10.97 MB de entrada y 18.44 MB de salida, en un intervalo de media hora. Por lo tanto el tráfico generado por un cliente será:

$$V_{\text{Entrada}} = \frac{10.79 \text{ MB}}{\text{muestra}} \times \frac{1 \text{ muestra}}{1800 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 49.1 \text{ kbps}$$

$$V_{\text{Salida}} = \frac{18.44 \text{ MB}}{\text{muestra}} \times \frac{1 \text{ muestra}}{1800 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 83.92 \text{ kbps}$$

2.3.5.1.3 Escritorio Remoto

Una sesión de escritorio remoto puede establecerse entre dos estaciones de trabajo o entre una estación y un servidor. El tráfico generado es similar al tráfico

del servicio de aplicaciones ya que estos dos servicios tienen tres características comunes: la interactividad, el protocolo utilizado y el patrón de tráfico. Por lo tanto, las velocidades estimadas para una sesión del servicio de aplicaciones serán similares a las de una sesión de escritorio remoto. Como máximo, existirán 2 sesiones simultáneas de escritorio remoto hacia el mismo equipo con una duración no mayor a dos horas.

2.3.5.1.4 Acceso a Internet ^[49]

Alianza de Seguros cuenta con un sistema de acceso a Internet controlado por el *firewall-proxy* Kypus, en el cual se encuentran configurados diferentes niveles de seguridad de acceso WEB, dependiendo de las características y necesidades de los empleados. Los empleados administrativos, gerentes y jefes de departamento, tienen todos los privilegios de acceso WEB; mientras que los empleados de operaciones y servicios tienen restringido el acceso y sólo pueden visitar páginas WEB autorizadas por el Departamento de Recursos Humanos (anexo F).

Para estimar el tráfico de acceso a Internet, se consideraron las páginas WEB más visitadas por los empleados administrativos, tomadas de los reportes del servidor Kypus. El tiempo de descarga y el tamaño promedio por página WEB visitada se midieron mediante una herramienta *online*.

Los resultados indican que la página WEB promedio tiene un tamaño de 537.34 KB, para la cual el tiempo de descarga promedio es de 23.6 segundos (ver anexo F). Este tiempo de descarga se considera aceptable y se lo mantendrá para el cálculo de la velocidad de acceso a Internet por usuario. Con estas bases se tiene que:

$$V_{descarga-WEB} = \frac{537.34KB}{página} \times \frac{1 página}{23,6 segundos} \times \frac{8 bits}{1 B} = 181.15 kbps$$

2.3.5.1.5 Correo Electrónico

El servicio de correo electrónico es proporcionado a todos los empleados que disponen de un computador. Está instalado en el servidor Kypus, donde se controlan cuentas de los usuarios y se maneja el espacio requerido para el almacenamiento de correo electrónico. El correo electrónico puede ser de tipo interno, entre usuarios del dominio segurosalianza.com, y externo, para otros dominios. También se tiene la posibilidad de adjuntar documentos, imágenes u otro tipo de archivos, siempre que no se exceda el tamaño límite.

El servidor Kypus tiene una herramienta de monitoreo de correo electrónico con la que se obtuvo un reporte del volumen de envío y recepción de correos en el intervalo de una semana. Los resultados se presentan en la tabla 2.39.

Los datos de la tabla 2.39 develan que el volumen de correo electrónico externo es menor que el tráfico de correo electrónico interno. También se observa que, a nivel externo, los usuarios tienden a enviar mayor cantidad de correos que los que reciben, mientras que a nivel interno los volúmenes de envío y recepción son similares.

	Volumen envío [GB]	Volumen recepción [GB]	Total volumen [GB]	Total Porcentaje
Externo	1,37	0,046	1,42	32%
Interno	1,27	1,69	2,96	68%
Total	2,64	1,74	4,38	100%

Tabla 2.39 *Volumen de información del servicio de correo electrónico en el intervalo de una semana*

El tráfico generado por el correo electrónico externo influye tanto en el enlace a Internet como en la red LAN, mientras que los correos electrónicos internos se manejan solo en la red LAN. Por lo tanto, para dimensionar los enlaces WAN y LAN se utilizará el tráfico de correo interno y externo mientras que para

dimensionar el enlace a Internet se utilizará únicamente el tráfico externo de correo electrónico.

Para proyectar la velocidad que requerirá este servicio es necesario tomar en cuenta el tamaño promedio de un correo electrónico. Para ello se consideró que el correo interno tiende a incluir texto e imágenes adjuntas, con un tamaño promedio de 100 KB por *mail*. El correo externo tiende a contener texto y archivos adjuntos, con un tamaño promedio de 350 KB. Se asume que en una hora se envía 1 correo externo y 3 internos aproximadamente. Con base en estas consideraciones se tiene:

Velocidad de correo electrónico interno:

$$V_{e-mail_interno} = \frac{100 \text{ KB}}{\text{mail}} \times \frac{3 \text{ mails}}{\text{hora}} \times \frac{1 \text{ hora}}{3600 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ B}} = 0.67 \text{ kbps}$$

Velocidad de correo electrónico externo:

$$V_{e-mail_externo} = \frac{350 \text{ KB}}{\text{mail}} \times \frac{1 \text{ mails}}{\text{hora}} \times \frac{1 \text{ hora}}{3600 \text{ seg}} \times \frac{8 \text{ bits}}{1 \text{ B}} = 0.78 \text{ kbps}$$

2.3.5.1.6 *Compartición de Archivos*

El servidor de archivos alberga diferente tipo de contenido: respaldos de *software*, archivos multimedia para diversos usos, hojas de cálculo, documentos de texto, etc. Este contenido es compartido por todos los usuarios pero sólo a nivel local. La compartición de archivos no está contemplada entre sucursales. La política de la empresa es tener un servidor de archivos en cada sucursal para contenido que sea propio de cada localidad.

La compartición de archivos es simple. Se trata únicamente de copiar archivos entre un computador y el servidor y solo requiere la orden del usuario para que la

transferencia se inicie. El tamaño típico de los archivos manejados en el servidor es de 4 MB y, dado que la transferencia se produce en el ambiente local, se suele utilizar todo el ancho de banda disponible en la copia de un archivo, siendo este servicio el principal causante de tráfico ráfaga. Sin embargo, en situaciones de alta carga, no se tolera más allá de 1 minuto para la copia de un archivo, para mantener la productividad empresarial.

Con estos parámetros, se tiene la siguiente velocidad de transmisión por archivo:

$$V_{Transferencia} = \frac{4 \text{ MB}}{\text{transferencia}} \times \frac{1 \text{ transferencia}}{60 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 546.13 \text{ kbps}$$

2.3.5.1.7 Video Vigilancia

Este servicio se ha requerido particularmente para las oficinas de Guayaquil-centro. Ya que las cámaras están conectadas directamente al servidor de video mediante cable coaxial, éstas no generan ningún tipo de tráfico en la red de datos. El tráfico se genera en la red cuando el administrador u otro usuario autorizado requieren monitorear lo que las cámaras están capturando. Para esto, el usuario debe usar un navegador WEB desde cualquier computador de la red y acceder al servidor de video; por lo tanto, el tráfico se transmite desde el servidor hacia el computador. El servidor de video envía el contenido capturado por las 4 cámaras simultáneamente hacia el computador y éste se despliega en la ventana del navegador WEB. El usuario puede cambiar este comportamiento para acceder al contenido de una sola cámara a la vez.

Cabe señalar que el servicio de video-vigilancia no necesita obtener la mejor calidad de imagen posible (comparable con televisión digital de alta definición), sino la calidad y velocidad de reproducción suficientes para poder distinguir personas y objetos con claridad y nitidez. Por esta misma razón el servicio de video-vigilancia no captura componentes de audio.

Para determinar el tráfico que genera el servicio de video-vigilancia, se debe conocer que el servidor trabaja con el estándar MPEG-4 (*Moving Pictures Experts Group-4*) para la transmisión de video y que soporta además los sistemas de video: PAL (*Phase Alternating Line*) y NTSC (*National Television System Committee*). En nuestro país el estándar de video utilizado es el NTSC.

En la tabla 2.40 se muestran el tamaño y velocidad de cuadro y la calidad de imagen soportada por el servidor; mientras que en la tabla 2.41 se muestra la velocidad de transmisión para ciertas combinaciones de tamaño, velocidad y calidad de imagen. Debido a que la velocidad de transmisión resultante en MPEG-4 depende del video capturado y otros múltiples factores, los valores mostrados en la tabla 2.41 son aproximados.

Tamaño de Cuadro [pixel]	Velocidad de Cuadro [IPS*]	Calidad de Imagen
720x480	30, 15, 7, 3	Mejor, Alta, Normal, Básica
720x240	60, 30, 15, 7	Mejor, Alta, Normal, Básica
352x240	120, 30, 15, 7, 3	Mejor, Alta, Normal, Básica

* IPS: Imágenes Por Segundo

Tabla 2.40 *Opciones de video disponibles en el servidor de video SRV Video para el sistema NTSC*

Tamaño de Cuadro [pixel]	Calidad de Imagen	Velocidad de Transmisión [kbps]	
		30 [IPS]	15 [IPS]
720x480	Alta	341	268
	Media	280	236
352x240	Alta	153	115
	Media	112	83.8

Datos obtenidos mediante el software *Ultra MPEG-4 Converter*

Tabla 2.41 *Velocidad de transmisión para diferentes combinaciones de video con MPEG-4.*

El ojo humano puede detectar una velocidad de cuadros por segundo de 30 IPS. No obstante, esta velocidad es excesiva para el servicio de video-vigilancia, donde se utilizarán solamente 15 IPS. Además, un cuadro de imagen de 352x240 píxeles permite distinguir claramente personas y objetos. Así que la combinación de tamaño y velocidad de cuadro para la transmisión de video configurada en el servidor será: 352x240@15IPS. Bajo estas condiciones, más una calidad de imagen media-alta, la velocidad de transmisión necesaria por cada cámara de video es aproximadamente de 115 kbps (ver tabla 2.41).

2.3.5.1.8 *Antivirus*

El tráfico del servicio de antivirus debe ser desglosado en dos partes. La primera, debido a las actualizaciones en el servidor principal y repositorios; la segunda, debido a las actualizaciones de los agentes. La actualización del servidor principal se realiza a través de la conexión de Internet. La actualización de los repositorios se realiza a través de los enlaces corporativos de la empresa. Y por último, las actualizaciones de los agentes se realizan en la red local (ver figura 2.8).

Los datos arrojados por el *sniffer* Wireshark sobre una actualización del servidor principal, indican que la cantidad de datos recibidos es de 108.78 MB y la cantidad de datos enviados es de 1.44 MB. Esta actualización, que será la misma para los repositorios, consta de las nuevas versiones del antivirus en sus diferentes versiones, agentes y sus parches para diferentes arquitecturas, y las bases de datos sobre virus.

Las actualizaciones se ejecutan una vez por semana, pero se requiere que se realicen en un lapso no mayor a una hora para mantener al servidor y a los agentes protegidos contra amenazas el mayor tiempo posible.

Con los datos obtenidos se puede estimar el tráfico entrante y saliente por las actualizaciones de antivirus en el servidor principal y repositorios:

Velocidad Entrada:

$$V_{\text{Entrada}} = \frac{108,78 \text{ MB}}{\text{actualización}} \times \frac{1 \text{ actualización}}{3600 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 247.53 \text{ kbps}$$

Velocidad Salida:

$$V_{\text{Salida}} = \frac{1,44 \text{ MB}}{\text{actualización}} \times \frac{1 \text{ actualización}}{3600 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 3.28 \text{ kbps}$$

Los agentes, instalados en cada computador de la red, obtienen sus actualizaciones desde el servidor principal, si están en la matriz; o desde los repositorios, si están en las sucursales. De esta manera se minimiza el tráfico circundante en la red. La diferencia entre las actualizaciones de servidores y agentes es el tamaño de la descarga. Los agentes necesitan únicamente las actualizaciones y parches para su versión específica de antivirus, y las bases de datos sobre virus. Es así que los datos descargados por el agente tienen un tamaño de 48.10 MB y los datos enviados un tamaño de 952.39 kB.

Esta actualización debe realizarse en un intervalo no mayor a media hora, antes de que los usuarios comiencen la jornada laboral.

Los requerimientos de velocidad por agente antivirus son los siguientes:

Velocidad Entrada:

$$V_{\text{Entrada}} = \frac{48,10 \text{ MB}}{\text{actualización}} \times \frac{1 \text{ actualización}}{1800 \text{ segundos}} \times \frac{1024 \text{ KB}}{1 \text{ MB}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 218.91 \text{ kbps}$$

Velocidad Salida:

$$V_{\text{salida}} = \frac{952,39 \text{ KB}}{\text{actualización}} \times \frac{1 \text{ actualización}}{1800 \text{ segundos}} \times \frac{8 \text{ bit}}{1 \text{ B}} = 4.23 \text{ kbps}$$

2.3.5.1.9 Llamada IP ^[33]

Los códecs G.711, G.722 y G.729 tienen velocidades de codificación de 64 kbps y 8 kbps respectivamente. El primero trabaja con 160 bytes por muestra de voz, mientras que el segundo usa 20 bytes (ver tabla 2.30). Debido a la sobrecarga que implica el añadir las cabeceras RTP/UDP/IP más la cabecera de la capa Enlace, el ancho de banda necesario para la transmisión será mayor que la velocidad de codificación.

Las cabeceras RTP/UDP/IP representan 40 bytes de sobrecarga. Sin embargo, con el uso de RTP comprimido (cRTP), estandarizado en el RFC 2508, se puede reducir la sobrecarga de las 3 cabeceras hasta 2 bytes.

El ancho de banda necesario por llamada IP, con compresión y sin compresión RTP, sigue la expresión:

$$AB_{\text{llamada IP}} = \frac{(\text{payload códec} + \text{cabeceras})}{(\text{payload códec})} \times \text{velocidad de codificación}$$

Para la red LAN se usarán los códecs G.711 y G.722, que tienen el mismo *payload* (tabla 2.30), más el protocolo de capa Enlace *Ethernet* IEEE 802.3 que añade 18 bytes de sobrecarga.

Ancho de banda sin compresión de cabecera:

$$AB_{\text{LANsc}} = \frac{(160 + 40 + 18) \text{ bytes}}{(160 \text{ payload}) \text{ bytes}} \times 64 \text{ kbps} = 87.2 \text{ kbps}$$

Ancho de banda con compresión de cabecera:

$$AB_{LANcom} = \frac{(160 + 2 + 18) \text{ bytes}}{(160 \text{ payload}) \text{ bytes}} \times 64 \text{ kbps} = 72 \text{ kbps}$$

Para el enlace WAN se usará el códec G.729 y el protocolo de capa *enlace Frame Relay*, que añade 4 bytes de forma general.

Ancho de banda sin compresión de cabecera:

$$AB_{WANcom} = \frac{(20 + 40 + 4) \text{ bytes}}{(20 \text{ payload}) \text{ bytes}} \times 8 \text{ kbps} = 25.6 \text{ kbps}$$

Ancho de banda con compresión de cabecera:

$$AB_{WANcom} = \frac{(20 + 2 + 4) \text{ bytes}}{(20 \text{ payload}) \text{ bytes}} \times 8 \text{ kbps} = 10.4 \text{ kbps}$$

Como se puede apreciar, la reducción de ancho de banda al usar compresión de cabecera no es significativa en redes LAN; por lo tanto se utilizará la opción sin compresión, que a su vez ayudará a reducir la carga de procesamiento. Por otra parte, en un enlace WAN con *Frame Relay*, el ancho de banda se reduce a la mitad al usar la compresión. En este caso, el uso de compresión es ventajoso por dos razones: menor consumo de ancho de banda en un enlace de capacidad limitada y la carga de procesamiento adicional debida al uso de compresión es baja ya que el número de llamadas simultáneas por el enlace WAN es reducido.

2.3.5.2 Ancho de Banda requerido según la simultaneidad de usuarios y servicios

El periodo estimado para este proyecto es de 5 años, tiempo para el cual es necesario conocer una aproximación del ancho de banda que requerirá la red. La proyección del tráfico permitirá determinar la capacidad a soportar por los enlaces

de los servidores y la capacidad máxima de *backbone* en las redes LAN de Quito y Guayaquil.

La red soportará los siguientes servicios principales: base de datos, correo electrónico, almacenamiento de archivos y Telefonía IP, para los cuales el usuario debe contar con un acceso rápido y sencillo. Un usuario puede hacer uso de todos los servicios simultáneamente, por lo que la capacidad de transmisión que requerirá será el resultado de la suma de las velocidades de acceso a cada uno de los servicios. Cada servicio tiene velocidades de entrada y salida diferentes. Como criterio de diseño para el dimensionamiento, se tomará en cuenta sólo la velocidad mayor y se asumirá que se requiere un canal simétrico. Es importante señalar que el servicio de Telefonía IP será tomado en cuenta como nuevo servicio de red, ya que compartirán recursos de red.

Para la proyección de tráfico del servicio de Telefonía IP se realizó preliminarmente un análisis tráfico de voz y códecs. Para el caso de la simultaneidad de este servicio se asumirá como caso crítico que todas las extensiones proyectadas realicen una llamada. En la tabla 2.42 se muestran, en resumen, el ancho de banda requerido para Telefonía IP en las redes LAN Quito y Guayaquil y el tráfico equivalente a 4 llamadas simultáneas para el enlace WAN entre las dos sucursales. El ancho de banda requerido por llamada para cada códec se asume sin compresión de cabecera RTP, como el peor de los casos.

Redes LAN			
Sucursal	# llamadas simultáneas*	Ancho de banda por llamada G.711 o G.722 [kbps]	Ancho de banda Telefonía IP [kbps]
Quito	50	87,2	4360
Guayaquil	30	87,2	2616
Enlace WAN Quito – Guayaquil			
# llamadas simultáneas	Ancho de banda por llamada G.729 [kbps]	Ancho de banda Telefonía IP [kbps]	
4	25.6	102.4	

* Valores según el número de usuarios proyectados de la tabla 2.37

Tabla 2.42 *Ancho de banda requerido para Telefonía IP en las redes LAN Quito y Guayaquil y enlace WAN*

Además de los servicios de red, es necesario conocer el número de usuarios simultáneos que se estima tener en cada servicio, el tipo de usuario y la capacidad necesaria para acceso de cada servicio. En la tabla 2.43 se muestra, en resumen, la proyección de tráfico para cada servicio de la red. Se incluye el servicio de video-vigilancia en esta tabla por ser de baja interactividad.

Servicio	V acceso x usuario [kbps]	Usuarios simultáneos actuales	Usuarios simultáneos proyectados	V acceso x servicio [kbps]
Base de Datos	9.953	71	79	786.287
Aplicaciones	83.92	2	5	419.6
Escritorio Remoto	83.92	2	2	167.84
Acceso a Internet	182.15	10	11	2003.65
Correo Electrónico*	1.45	5	6	8.7
Compartición de Archivos	546.13	5	6	3276.78
Video vigilancia	115	1	1	115
Antivirus	218.91	5	6	1313.46
Complementarios	168.96	15	17	2872.32
Telefonía IP**	87.2	45	50	4360
TOTAL x USUARIO	1497.59			

* Este valor se obtiene sumando el tráfico de correo interno y externo de la página 143.

**Telefonía IP contiene el cálculo referencial para los usuarios de Quito, en la tabla 2.44 se muestra el resumen para el *backbone* tanto de Quito como de Guayaquil.

Tabla 2.43 *Proyección de tráfico en 5 años para cada servicio de datos*

De lo mostrado en la tabla anterior, el número de usuarios simultáneos actuales fue obtenido en base a una herramienta de monitoreo para los servicios de Base de datos y Antivirus; en el caso de los servicios de compartición de archivos y aplicaciones este número se observó mediante la herramienta de rendimiento del sistema operativo del servidor. Por último, la concurrencia de usuarios para el servicio de acceso a Internet y correo electrónico es aproximada.

El número de usuario se estimó en base al 10% de crecimiento que se espera tener en los próximos 5 años, con excepción del servicio de aplicaciones que, según información del Departamento de Sistemas, se plantea incrementar a cinco unidades más por los réditos productivos gracias a los equipos *Thin-Client*.

El valor de 1497.54 kbps, mostrado en la tabla 2.43, es el máximo ancho de banda que un usuario podría requerir para acceder a todos los servicios. Aunque es poco probable que cada empleado acceda simultáneamente a todos los servicios, este evento debe ser tomado en cuenta para el dimensionamiento de los terminales por ser el peor de los casos.

2.3.5.3 Ancho de banda estimado para *backbone* de las redes LAN Quito y Guayaquil

Una vez conocidos los valores de ancho de banda requeridos para cada servicio que correrá en la red corporativa, se puede estimar el ancho de banda requerido para el *backbone* de cada red LAN, como se muestra en la tabla 2.44.

Servicio	Ancho de Banda [kbps]
Base de Datos	786.287
Aplicaciones	419.6
Escritorio Remoto	167.84
Acceso a Internet	2003.65
Correo Electrónico	8.7
Compartición de Archivos	3276.78
Video vigilancia	115
Antivirus	1313.46
Complementarios	2872.32
TOTAL DATOS	10963.94
Telefonía IP Quito*	4360
Telefonía IP Guayaquil*	2616
BACKBONE Quito	15323.94
BACKBONE Guayaquil	13579.94

* Valores tomados de la tabla 2.42

Nota: Para el *backbone* de Guayaquil se consideró la probable redundancia de servicios de datos de Quito como el peor de los casos.

Tabla 2.44 *Ancho de banda para backbone en redes LAN Quito y Guayaquil*

Los datos de la tabla 2.44 indican que el ancho de banda requerido en la ciudad de Quito sólo para datos es de 10.96 Mbps. Si además se toma en consideración el ancho de banda requerido para Telefonía IP, se tienen 15.32 Mbps requeridos para Quito y 13.58 Mbps requeridos para Guayaquil. Estas cifras son bajas si se

las compara con los cientos de Mbps que están en capacidad de soportar las actuales tecnologías de redes LAN, como es *Fast Ethernet*.

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 2

LIBROS

- [65] HELD Gilbert. "Ethernet Networks. Design, Implementation, Organization & Management". Cuarta Edición. Edit. John Wiley & Sons 2003.
- [66] LIN Weisi. "Multimedia Analysis. Processing and Communications". Edit. Springer 2011
- [67] KATZ Marcos D. "WiMAX Evolution: Emerging Technologies and Applications". Primera Edición. John Wiley & Sons 2009

INTERNET

- [68] Seguros Alianza.
<http://www.segurosalianza.com/>
- [69] Información básica. ¿Qué es el SLA?
http://www.acens.com/file_download/176
- [70] IBM Personal Communications Version 5.7 for Windows operating systems
<http://publib.boulder.ibm.com/infocenter/pcomhelp/v5r9/index.jsp?topic=/com.ibm.pcomm.doc/readme/readV57.html>
- [71] IBM System 515i Express
<ftp://public.dhe.ibm.com/common/ssi/pm/sp/n/isd03001usen/ISD03001USEN.PDF>
- [72] Centro de Información de DB2
<http://publib.boulder.ibm.com/infocenter/db2luw/v8/index.jsp>
- [73] DB IBM DB2
http://en.wikipedia.org/wiki/IBM_DB2
- [74] McAfee Agent 4.5 Product Guide

- http://download.nai.com/products/naibeta-download/epo_450/ma_450_relcandidate_productguide.pdf
- [75] McAfee Agent Handler
http://www.nwtechusa.com/pdf/mcafee_epo_wp.pdf
- [76] McAfee ePolicy Orchestrator 4.0
http://download.nai.com/products/protected/epo/version_4.0.0/spanish/epo_400_installguide_es-es.pdf
- [77] McAfee ePolicy Orchestrator 4.5 Product Guide
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/21000/PD21812/en_US/epo_450_product_guide_en-us.pdf
- [78] McAfee VirusScan Enterprise 8.7i Product Guide
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/20000/PD20690/en_US/vse_870_product_guide_en-us.pdf
- [79] Kypus *Thin-Client*. "La nueva generación de *Thin-Client*"
http://www.novadevices.com/images1/ktc_white_paper.pdf
- [80] Kypus *Thin-Client*. Especificaciones
http://www.novadevices.com/images1/brochure_XP2.pdf
- [81] XP Unlimited
http://www.neogenesys.com.mx/Spanish/Catalogo/Clientes_Ligeros/XP_Unlimited/xp_unlimited.htm
- [82] XP Unlimited
<http://www.infomat.es/xpunlimited.html>
- [83] VNC® Enterprise Edition 4.5 - Release Notes
<http://www.realvnc.com/products/enterprise/4.5/release-notes.html>
- [84] Protocols and Interfaces to Active Directory
<http://technet.Microsoft.com/en-us/library/cc961766.aspx>
- [85] Best Digital Security Guard Series
http://www.wecl.com.hk/digiguard/DIGIguard.files/DIGI_manual_V0.9.pdf
- [86] Understanding NetBIOS and Windows Server 2003
<http://oreilly.com/pub/a/windows/2004/05/11/netbios.html>

- [87] How To Configure TCP/IP Networking While NetBIOS Is Turned Off on a Server Running Windows Server 2003
<http://support.Microsoft.com/default.aspx?scid=kb;en-us;323357>
- [88] MEGADATOS S.A., Ecuador
<http://www.megadatos.com/>
- [89] IP-Adress. "DNS"
http://www.ip-adress.com/ip_tracer/64.46.64.254
- [90] Consulta de dominio. "DNS"
<https://secure.domain.com/services/whois.php>
- [91] Understanding NetBIOS and Windows Server 2003
<http://oreilly.com/pub/a/windows/2004/05/11/netbios.html>
- [92] Terra, "Tráfico Telefónico"
http://www.terra.es/personal/ignaciorb/telefonía/conmutacion/conmutacion_2.htm
- [93] Panasonic. Digital Super Hybrid System. Installation Manual. KX-TD1232
<http://pdf.textfiles.com/manuals/TELECOM-F-R/Panasonic%20KX-TD1232%20Installation.pdf>
- [94] Panasonic. Digital Super Hybrid System. User Manual. KX-TD1232
<http://www.compucanj.es/manuales/td1232-816.pdf>
- [95] Manual de instrucciones Alcatel 4200 E .
http://sumanual.com/instrucciones-guia-manual/ALCATEL-LUCENT/4200%20E-_F
- [96] IP Telephony Design Guide. Alcatel White Paper.
http://www.connect802.com/download/general/Alacatel_VoIP_Design_Guide.pdf
- [97] Voice Over IP - Per Call Bandwidth Consumption
http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml
- [98] Wideband Audio and IP Telephony
http://cisco.biz/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8537/prod_white_paper0900aecd806fa57a.html
- [99] Pulse Code Modulation (PCM) of Voice Frequencies ITU-T G.711
<http://www.analytic.ru/articles/lib228.pdf>

- [100] Coding of speech at 16 kbit/s using low-delay code excited linear prediction
ITU-T G.728
<http://www.ece.cmu.edu/~ece796/documents/g728e.pdf>
- [101] 7 kHz audio-coding within 64 kbit/s
<http://neutron.ing.ucv.ve/comunicaciones/Asignaturas/DifusionMultimedia/T-REC-G.722-198811-III!PDF-S.pdf>
- [102] Introduction to CELP Coding
<http://www.speex.org/docs/manual/speex-manual/node9.html>
- [103] A comparison of speech coding algorithms: ADPCM vs CELP
<http://www.utdallas.edu/~torlak/wireless/projects/wichman.pdf>
- [104] Quality comparison of wideband coders including tandeming and transcoding
http://portal.etsi.org/stq/workshop2007presentations/Quinquis_slides.pdf
- [105] RTP Payload Format for the G.729.1 Audio Codec
<http://www.ietf.org/rfc/rfc4749.txt>
- [106] Voice
<http://www.rhyshaden.com/voice.htm>
- [107] Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation
http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml
- [108] Analyzing of MOS and Codec Selection for Voice over IP Technology
<http://anale-informatica.tibiscus.ro/download/lucrari/7-1-27-Mohd.pdf>
- [109] Recommendation G.729.1
<http://www.itu.int/rec/T-REC-G.729.1/en>
- [110] Recommendation G.722
<http://www.itu.int/rec/T-REC-G.722/e>
- [111] Next-generation VoIP and the role of DSP
<http://www.eetimes.com/design/signal-processing-dsp/4017493/Next-generation-VoIP-and-the-role-of-DSP?pageNumber=0>
- [112] Wideband IP Phones
<http://www.voip-info.org/wiki/view/WideBandIPPhones>

- [113] Herramienta WEB de medición de tiempo de descarga de páginas WEB
<http://tools.pingdom.com/>
- [114] Calculadora Erlang
<http://personal.telefonica.terra.es/WEB/vr/erlang/index.htm>

PROYECTOS DE TITULACIÓN

- [115] CEVALLOS Gabriel, TASINTUÑA Luis. "Diseño de una red integrada de voz y datos para el campus E.P:N. Basado en un análisis comparativo de las soluciones existentes en el mercado nacional". Quito. mayo 2007. Cap 2. pag 124-140

CAPÍTULO 3

DISEÑO DE LA RED DE DATOS Y TELEFONÍA IP, SOLUCIONES DE TELEFONÍA IP

Como etapa preliminar se realizó el análisis de la situación actual de las redes de datos y de voz, obteniéndose los requerimientos necesarios para presentar una solución que permita integrar el servicio de Telefonía IP a la red corporativa de Alianza de Seguros. Como solución se plantea la reingeniería de la red de datos para la integración de los servicios de Telefonía IP, la misma que permitirá mejorar el rendimiento y la disponibilidad actuales de la red; además proporcionará mayor escalabilidad, seguridad y facilidades en la administración.

Como parte de este capítulo se analizarán las posibles soluciones de Telefonía IP para Alianza, de acuerdo al mercado nacional actual. Se analizarán las soluciones de Telefonía IP presentadas por fabricantes tradicionales de conectividad como CISCO y HP/3COM⁵, y la de fabricantes de Telefonía tradicional como AVAYA. Cada uno de ellos brinda soluciones integrales de Telefonía IP a sus clientes.

Finalmente, se resumirán las características de los materiales y equipos requeridos, que se determinan a lo largo del desarrollo del presente capítulo.

3.1 ESQUEMA DE REINGENIERÍA PROPUESTO

El proceso de reingeniería empezará por definir los elementos, funcionamiento y dimensionamiento básicos para las redes LAN de las agencias de Quito y Guayaquil⁶. Además de la reorganización de los servicios existentes en la red, se indicará el funcionamiento y el dimensionamiento para los servicios de Telefonía

⁵ HP absorbió a la empresa 3COM en el año 2010.

⁶ Guayaquil cuenta con dos agencias, una en el centro de la ciudad y otra en el sector de la Kennedy. Cuando se mencione a Guayaquil en este capítulo, se referirá a la agencia del centro a menos que se especifique lo contrario.

IP. Luego se continuará con el dimensionamiento del enlace WAN entre las dos agencias y el acceso a servicios externos. Posteriormente se definirán las características y elementos necesarios para proveer calidad de servicio, disponibilidad, administración y seguridad a lo largo de la red corporativa.

3.1.1 MODELO JERÁRQUICO ^{[1][2]}

El diagrama de la figura 3.1 muestra el esquema en el que se basará la reingeniería de la red corporativa de Alianza de Seguros. Se considerarán los siguientes elementos: las redes LAN de Quito y Guayaquil, el enlace WAN entre estas dos sucursales y los respectivos accesos a servicios externos como la Internet y la PSTN, todos ellos organizados dentro del modelo jerárquico.

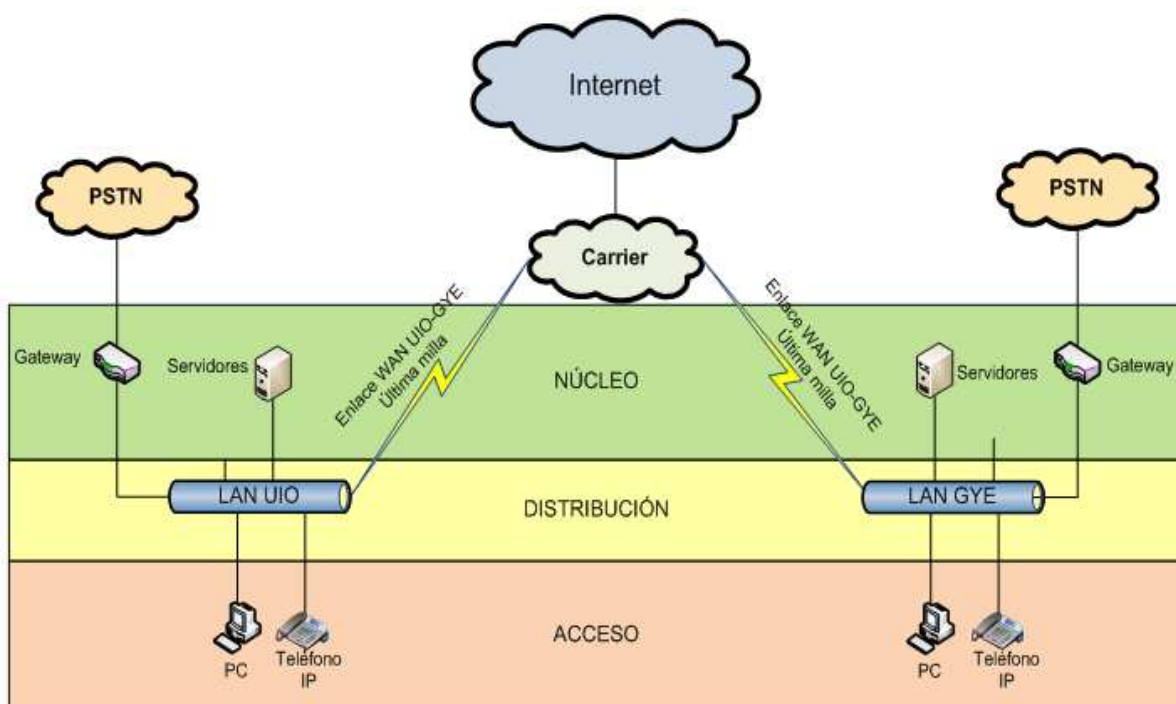


Figura 3.1 *Esquema general para el diseño de red propuesto*

El modelo jerárquico es ampliamente utilizado en diseño de redes, porque al ser modular, presenta beneficios en aspectos tales como: escalabilidad, administración, rendimiento y costo-beneficio. Esto se consigue al dividir a la red, según sus funciones, en 3 capas: acceso, distribución y núcleo.

La capa de acceso está destinada a que los usuarios se conecten a la red e interactúen con ella. En este nivel se encontrarán los dispositivos terminales de usuario como computadores, teléfonos IP, impresoras, máquinas de fax o también otros equipos de conectividad como puntos de acceso inalámbricos para dispositivos móviles. En esta capa se puede agrupar a los usuarios por departamento o funciones y también permite establecer qué dispositivos terminales tendrán o no acceso a la red. El número de equipos de conectividad necesarios en esta capa será proporcional al número de dispositivos terminales que se utilizarán.

No todos los recursos de la red están al alcance directo del usuario en la capa acceso. La capa de distribución servirá de intermediario entre la capa de acceso y la capa de núcleo. En esta última es donde se encontrarán básicamente los servicios de la red. Las funciones principales de la capa distribución son: enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo, segmentar la red en múltiples dominios de difusión, servir como punto de concentración para acceder a los dispositivos de usuario y proporcionar seguridad mediante filtrado y control de acceso. Esta capa determina cuál es la forma más rápida para que la petición de un usuario pueda ser remitida al servicio requerido. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo.

En general, la capa de núcleo es responsable de transportar grandes volúmenes de información de manera rápida y confiable. En esta capa también se considerará el acceso a los servicios internos, como la base de datos o Telefonía IP, y servicios externos, a través del acceso WAN y la PSTN.

Del tráfico que cruza por las capas de distribución y núcleo dependen todos los usuarios, así que si alguna de estas capas falla, cada uno de los usuarios se puede ver afectado. Por esta razón, estas dos capas merecen especial atención en el diseño, y se debe considerar el uso de algún esquema de redundancia que garantice el acceso a los servicios.

3.2 DISEÑO DE LAS REDES LAN QUITO Y GUAYAQUIL CON SERVICIOS INTEGRADOS DE TELEFONÍA IP ^[2]

Por razones estratégicas de la empresa, los principales servicios se brindan desde la matriz en Quito, razón por la cual esta red debe estar en condiciones de soportar la carga que estos servicios suponen. Para ello, se procederá a realizar el diseño del cableado estructurado de la matriz, para luego continuar con la conectividad y los servicios de las agencias de Quito y Guayaquil, incluida la Telefonía IP. Como se ha visto en el capítulo 2, la red se diseñará para un crecimiento de 5 años, con la única excepción del cableado estructurado, para el cual los estándares exigen que su tiempo de vida útil sea de al menos 10 años.

En este diseño de red se utilizará topología en estrella y las tecnologías de redes conmutadas *Ethernet* (IEEE 802.3i, 10 Mbps), *Fast Ethernet* (IEEE 802.3u, 100 Mbps) y *Gigabit Ethernet* (IEEE 802.3ab, 1000 Mbps) para dispositivos de usuario y *uplinks*. Estas tecnologías serán soportadas con cableado estructurado de cobre categoría 6. Estas tecnologías se han seleccionado en base al análisis de requerimientos, en el que se determinó que los volúmenes máximos de tráfico no superan su capacidad. Adicionalmente, estas tecnologías son las que mejor se adaptan a las condiciones físicas que presentan las instalaciones, como distancias máximas, número de pisos, densidad de usuarios, etc.

3.2.1 SISTEMA DE CABLEADO ESTRUCTURADO PARA QUITO ^{[4][5][22]}

Se tomará como base los estándares EIA/TIA 568 para instalación de cableado, EIA/TIA 569A para rutas y espacios de telecomunicaciones, EIA/TIA 606 para la administración del sistema de cableado, presentada más adelante en la sección de administración, y EIA/TIA 607 para la puesta a tierra; estas normas se adaptarán a la infraestructura particular de este proyecto.

A continuación se detallarán las condiciones y el diseño de las 5 áreas definidas para el sistema de cableado estructurado: áreas de trabajo, cuarto de equipos, cuarto de telecomunicaciones, cableado horizontal y cableado vertical.

3.2.1.1 Áreas de Trabajo ^[24]

Considerando la norma TIA/EIA 569-A que define a las áreas de trabajo como los espacios de un edificio en donde los ocupantes interactúan con los dispositivos de telecomunicaciones, se procedió a dividir las diferentes áreas de trabajo de cada departamento.

Para el establecimiento de las áreas de trabajo del edificio de Alianza Quito, se tomó como referencia los actuales puestos de trabajo ubicados en cada departamento y los posibles lugares donde se prevé podrían ir ubicadas otras áreas en el futuro.

Se dispondrá de dos salidas de telecomunicaciones por área de trabajo, una para datos y otra para voz. Las áreas donde se encuentran impresoras y faxes tendrán una sola salida ya sea para datos ó voz dependiendo del caso. En áreas muy particulares se dispondrá de salidas dobles para datos ó voz, debido a que se requieren hasta dos impresoras de red ó dos terminales telefónicos en el mismo lugar.

En la tabla 3.1 se resume por piso la cantidad de puntos de datos y voz que se tendrán. La distribución física de los puntos de voz y datos se incluyen en los planos del anexo G.1.

Cada área de trabajo contendrá los *face-plates* necesarios sujetos a la pared, de una y dos salidas dependiendo del área. En ellos se sujetarán los *jacks* RJ-45 para conexión con los *path-cords* UTP de 2 metros. La terminación de los pares trenzados a ser usada en los conectores RJ-45, seguirá el estándar T568B, ilustrada en la figura 3.2.

3.2.1.2 Cuarto de Equipos ^[25]

El cuarto de equipos es definido como el espacio donde se ubicarán equipos de servicios o telecomunicaciones.

El cuarto de equipos se mantendrá en el Departamento de Sistemas, primer piso, ya que brinda las condiciones de seguridad física requeridas. Además, se consideró que el lugar presenta las características adecuadas que son recomendadas por la norma TIA/EIA 569-A, entre las que se encuentran:

- Altura mínima de 3 metros.
- No existen tuberías de agua alrededor o sobre el cuarto de equipos.
- El sistema de puesta a tierra actual cumple con la norma ANSI/TIA/EIA 607.
- El actual cuarto de equipos dispone de un sistema con llave para el acceso, dispuesto únicamente para el personal autorizado de Sistemas.
- Se cuenta con un UPS como respaldo de energía y aire acondicionado como sistema de climatización. Sin embargo, estos elementos se redimensionarán más adelante en la sección de disponibilidad, después de obtener los requerimientos de potencia de los nuevos equipos que se añadirán.

Piso	Puntos de Datos	Puntos de voz
SB	29	25
PB	20	22
P1	22	21
P2	2	2
PI*	4	5
TOTAL	77	75

*PI: Planta independiente, Extern-Solut, Suite y Guardianía.

Tabla 3.1 *Resumen de Puntos de datos y voz por piso*

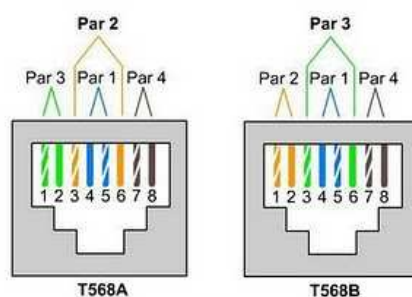


Figura 3.2 *Estándares T568A y T568B para conectores RJ-45*

El cuarto de equipos servirá también como terminación del cableado horizontal para el primer piso y la planta baja, debido a la falta de espacios adecuados para el cuarto de telecomunicaciones en el piso inferior. En cualquier caso, se ha tomado en cuenta que no se sobrepasen las distancias máximas permitidas para los cables y que exista el espacio necesario para las rutas de cables, tal como se verá en las secciones de cableado horizontal y cableado vertical.

3.2.1.3 Cuarto de Telecomunicaciones ^[26]

El cuarto de telecomunicaciones es el área dentro de un edificio donde termina el cableado horizontal y se interconecta el cableado vertical; el mismo que puede albergar equipamiento de telecomunicaciones.

En los cuartos de telecomunicaciones especificados se dispondrán *switches* que servirán como acceso a la red, y *patch panels* (figura 3.3) donde se concentrará el cableado horizontal del área de servicio. En el anexo G.2 se especifica el dimensionamiento de cada uno de los *racks*.



Figura 3.3 *Patch panel*

El subsuelo contará con un cuarto de telecomunicaciones ubicado en la parte central del área a la que sirve. En el caso de la planta independiente, se tendrá únicamente un *rack* cerrado, debido al reducido número de puntos en esta área.

Según la norma TIA/EIA 569-A se debe tener como mínimo un cuarto de telecomunicaciones por piso. Por motivos estructurales, se consideró un solo cuarto de telecomunicaciones por cada dos pisos debido a que el área a servir y el número de puntos de red son reducidos.

Los cuartos de equipos y telecomunicaciones se encontrarán repartidos como se indica en la figura 3.4.

3.2.1.4 Cableado Horizontal

El cableado horizontal lo constituyen todos los elementos que permiten la llegada del cableado desde el *rack*, en el cuarto de telecomunicaciones, a la salida de telecomunicaciones en el área de trabajo.

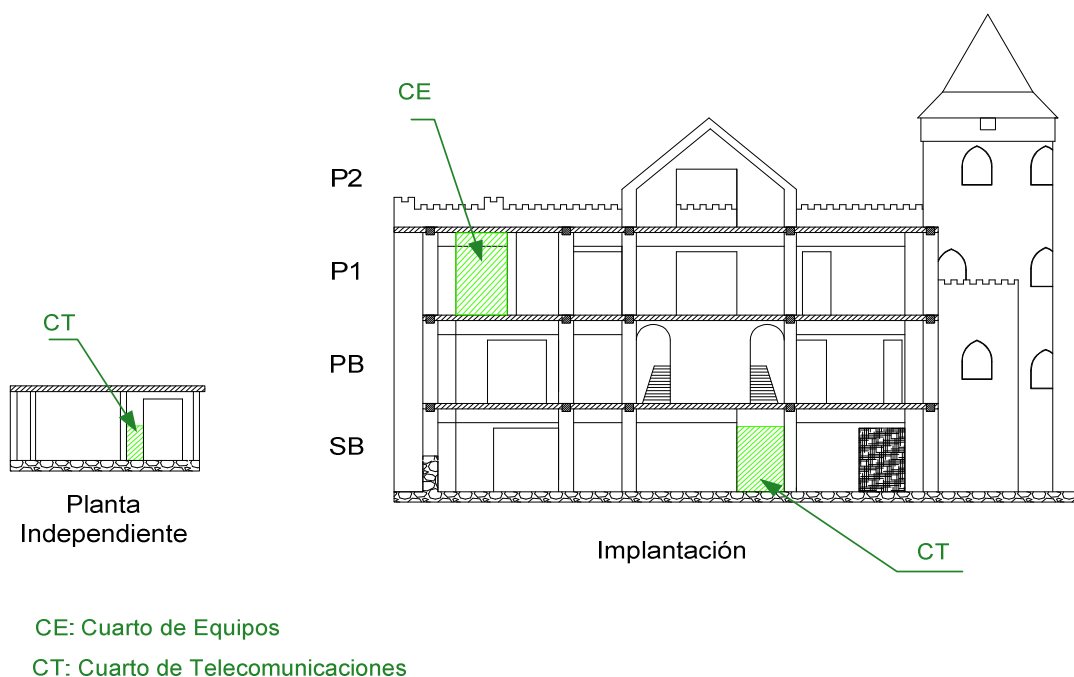


Figura 3.4 *Distribución de los cuartos de equipos y de telecomunicaciones*

3.2.1.4.1 Categoría a Utilizar^{[27]-[30][31]}

La estimación del crecimiento de la red ha permitido establecer un cálculo aproximado del tráfico que tendrá que soportar la red en 10 años. Para el presente proyecto, se determinó que en 10 años el tráfico producido por un sólo usuario no superará la velocidad de 10 Mbps producto de sus labores empresariales. Por ello es suficiente el uso de la categoría 5e para el cableado horizontal que permite soportar una velocidad de 100 Mbps. Por otra parte, se conoce que la categoría 5e hoy en día está siendo reemplazada por la categoría 6 (250 MHz), debido al dinamismo de las redes y a la aparición de nuevas

aplicaciones, sobre todo de tipo multimedia. Por esta razón, en este diseño se considerará el uso de la categoría 6, incluyendo: cable UTP, *jacks* y *plugs* RJ-45, *patch cords*, y accesorios pertinentes, ilustrados en la figura 3.5.

El cable UTP a utilizarse como parte del cableado horizontal será del tipo CMP (*Communications Plenum Cable*). Este tipo de cable se utiliza para rutas donde existe circulación de aire, como es el caso del cielo raso, para evitar la propagación de incendios.

a) *Face-plate*b) *Jack* RJ-45c) *Plug* RJ-45d) *Patch Cord*

Figura 3.5 *Elementos de cableado estructurado en el área de trabajo*

3.2.1.4.2 *Rutas de Cableado*

La mayoría de oficinas del edificio cuenta con la facilidad de techo falso, el cual se usará como ruta principal de distribución para el cableado horizontal. Sobre él se ubicarán escalerillas para la mayor densidad de cable y tubería *Conduit* EMT (*Electrical Metallic Tubing*), con sus respectivos accesorios.

Existen rutas que forzosamente deben atravesar algunas paredes por encima del techo falso. Sin embargo, las paredes están construidas en su mayoría con bloque y las rutas evitarán en su trayectoria a columnas y luminarias.

Las rutas que llegan hasta el *face-plate* en cada área de trabajo, estarán formadas por canaletas decorativas sobre las paredes, utilizando elementos adicionales como ángulos internos y externos, codos, esquineros, acopladores reductores, etc.

El cableado horizontal de la planta baja será terminado en el cuarto de equipos del primer piso como se dejó indicado. La distancia medida desde el punto de red más lejano en la planta baja hasta el cuarto de equipos del primer piso es de 48.04 metros, que no excede el límite de 90 metros estipulado por las normas. Los 4 puntos existentes en el segundo piso terminarán en el cuarto de equipos.

El punto de voz existente en la guardianía, fuera del edificio principal, se seguirá manteniendo con par de cobre telefónico. Este punto utilizará un ATA (*Analog Telephone Adapter*) para integrarse al sistema de Telefonía IP.

3.2.1.5 Cableado Vertical

El cableado vertical o *backbone* es aquel que permite la conexión entre los distintos cuartos de telecomunicaciones.

3.2.1.5.1 Categoría a Utilizar^[31]

Para este diseño se estima que la capacidad proyectada de *backbone* requerida para el tráfico no sobrepasará los 100 Mbps. Sin embargo, se hará uso de cable categoría 6 por razones de compatibilidad con nuevas aplicaciones posibles en el futuro y por compatibilidad con la categoría del cableado horizontal.

Para el cableado vertical se utilizará cable UTP tipo CMR (*Communications Riser Cable*), por ser el que se utiliza en instalaciones entre pisos por ser ductos donde no hay mucha circulación de aire.

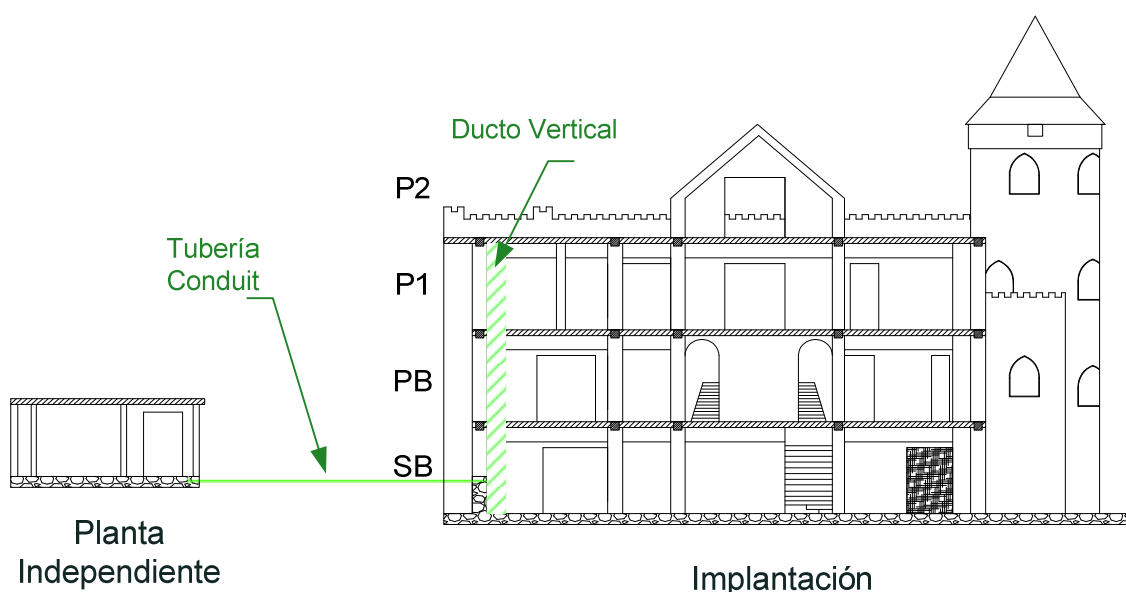
3.2.1.5.2 Rutas de Backbone

El *backbone* estará conformado por dos tipos de rutas: una interna y otra externa.

Dentro del edificio se tiene un ducto vertical que atraviesa la estructura desde el subsuelo hasta el primer piso. Este ducto se utilizará como ruta para el cableado

vertical; en él se colocarán dos tuberías *Conduit* EMT de 3 pulgadas con una capacidad de hasta 40 cables UTP categoría 6 cada uno. La cantidad máxima de cables que contendrán entre las dos tuberías es de 48 cables UTP: 42 para los puntos de red de la planta baja más 6 cables de *backbone* (3 utilizados y 3 de respaldo). De esta manera se tiene un espacio disponible en las tuberías para albergar 32 cables adicionales.

La interconexión entre la planta independiente y el edificio principal consta de una tubería *Conduit* enterrada que une el suelo de la planta independiente con la pared lateral de la planta baja del edificio principal, empalmándose con el ducto antes mencionado. En la figura 3.6 se aprecian las rutas para el cableado vertical. Todos los elementos del cableado estructurado contemplarán el uso de material retardante de fuego para evitar la propagación de incendios.



Nota: El desnivel observado entre estructuras es propio de la construcción

Figura 3.6 *Rutas de Cableado Vertical*

3.2.1.6 Dimensionamiento de los elementos para el Cableado Estructurado

Los materiales principales a ser utilizados para el sistema de cableado estructurado son: escalerillas galvanizadas, tubería *Conduit* EMT y canaletas para

las rutas del cableado; cable UTP categoría 6 y accesorios para el cableado horizontal y vertical; y por último, los *racks* y sus accesorios para el cuarto de equipos y de telecomunicaciones.

3.2.1.6.1 Dimensionamiento de elementos para Rutas de Cableado ^[4]

Los principales criterios para el dimensionamiento de las rutas son el área de sección del cable a utilizar y el radio de curvatura de las rutas. El cable UTP categoría 6 que se comercializa tiene un diámetro que se encuentra entre 5.9 mm (marcas Panduit y Siemon) y 6.12 mm (marca Belden). La tabla 3.2 muestra la cantidad máxima de cables de 6.1 mm que se pueden colocar al interior de una tubería *Conduit*, según la norma TIA/EIA 569A.

Para otras rutas, como escalerillas y canaletas, la norma dicta que la capacidad a utilizar es del 40% al momento de la instalación, alcanzando un máximo del 60% con adiciones futuras. La tabla 3.3 muestra el resumen de la capacidad de escalerillas y canaletas estándar para el cable empleado.

De igual manera, la norma TIA/EIA 569 A establece que el radio de curvatura mínimo para el cable UTP debe ser de 4 veces su diámetro. Los fabricantes disponen de los accesorios necesarios para el cumplimiento de la norma.

Conduit		Máximo Número de Cables UTP
Denominación [pulgadas]	Diámetro Interno [mm]	6.1 [mm]
½	15,7	0
¾	20,8	3
1	26,7	6
1 ¼	35	10
1 ½	40,9	15
2	52,6	20
2 ½	62,7	30
3	80	40

Tabla 3.2 Capacidad de Tubería *Conduit* para cable UTP de 6.1 mm de diámetro según norma ANSI-EIA/TIA 569 A

Ducto	Medidas		Área		Número de cables UTP CAT 6 6.1 [mm]	
	Ancho [mm]	Alto [mm]	[mm ²]	[pulg ²]	40%	60%
Escalerilla	300	100	30000	46.50	397	596
	150	100	15000	23.25	199	298
Canaleta	13	7	91	0.14	1	2
	20	12	240	0.37	3	5
	30	12	360	0.56	5	7
	40	25	1000	1.55	13	20
	60	40	2400	3.72	32	48
	100	45	4500	6.98	60	89

Tabla 3.3 Capacidad de escalerillas y canaletas estándar para cables UTP de 6.1 mm de diámetro

3.2.1.6.2 Cálculo del número de rollos de cable

Para calcular el número total de rollos de cable UTP necesarios para el diseño del cableado estructurado existen dos métodos: medir todas las distancias de las corridas de cable (método exacto), o hacer una estimación en base a una fórmula estandarizada (método aproximado). Las distancias de los puntos de red del presente diseño de cableado estructurado se adjuntan en el anexo G.3. A continuación se muestran los pasos a seguir para realizar el cálculo del número de rollos con la fórmula estandarizada. Como el edificio en cuestión es relativamente pequeño, se realizará un único cálculo de rollos para todo el edificio, para así evitar el desperdicio de cable.

1. Tomar la distancia a los puntos de red más lejano (d_{max}) y más cercano (d_{min}) al cuarto de telecomunicaciones, y sacar el promedio (d_{med}).

$$d_{max} = 46.11 [m]$$

$$d_{min} = 0.72 [m]$$

$$d_{med} = \frac{d_{max} + d_{min}}{2} = \frac{46.11 + 0.72}{2} = 23.41 [m]$$

2. Ajustar la distancia promedio (d_{med}), aumentando un 10% de holgura.

$$d_{ajd} = d_{med} + 10\% = 23.41 + 2.34 = 25.76 \text{ [m]}$$

3. Calcular el número de corridas por caja o rollo de cable UTP, dividiendo la longitud total de un rollo ($L = 305$ m, medida estándar) para la distancia promedio ajustada, y redondear hacia el número entero menor.

$$\# \text{ corridas} = \frac{L}{d_{ajd}} = \frac{305}{25.76} = 11.84 \Rightarrow 11 \text{ corridas}$$

4. Calcular la cantidad de cajas o rollos, dividiendo el número de puntos de red (n) para el número de corridas, y aproximar al número entero mayor.

$$\# \text{ rollos} = \frac{n}{\# \text{ corridas}} = \frac{152}{11} = 13.81 \Rightarrow 14 \text{ rollos}$$

Al aplicar el método exacto, midiendo todas las distancias de los puntos más un 10% de seguridad, se obtienen 13 rollos requeridos, mientras que con el método aproximado se obtienen 14 rollos. Como la diferencia entre los métodos es apenas de un rollo, se comprueba que el método aproximado es rápido y a la vez confiable.

El detalle del número total de rollos de cable UTP categoría 6 tipo CMP, que se utilizará en el cableado horizontal, se muestra en la tabla 3.4.

Planta	# Puntos	dmax [m]	dmin [m]
Subsuelo	54	37.97	7.37
Planta Baja	42	46.11	17.3
Primer Piso	43	28.71	9.4
Segundo Piso	4	37.39	24.62
Planta Independiente	9	8.66	0.72
Puntos totales	152		

Número de rollos totales	14
---------------------------------	-----------

Tabla 3.4 *Rollos de cable UTP cat 6 necesarios para el cableado horizontal*

Se utilizará un rollo de cable UTP categoría 6 tipo CMR para el cableado vertical ya que la longitud total necesaria es inferior a los 305 m totales del rollo. El detalle de cable UTP para cableado vertical se muestra en la tabla 3.5.

	Cantidad Enlaces	Longitud Enlace [m]	Longitud Total [m]
Cable UTP interno	2	39.21	78.42
Respaldo	2	39.21	78.42
Cable UTP externo	1	31.18	31.18
Respaldo	1	31.18	31.18
Subtotal			219.2
Seguridad +10%			21.92
TOTAL			241.12

Tabla 3.5 *Detalle de cable UTP para cableado vertical*

3.2.2 DISEÑO DE LA RED ACTIVA DE QUITO Y GUAYAQUIL

El diseño de la red activa combina la red de datos y la red de voz en la misma infraestructura. En el presente diseño se especifican los elementos activos de red a utilizarse, la interconexión de estos elementos y el diseño lógico propuesto para la red.

3.2.2.1 Elementos Activos de la Red

La red activa está compuesta de los siguientes elementos: terminales de usuario, servidores y equipos de conectividad. Se conectarán mediante variantes de la tecnología *Ethernet*, ya que cumple con los requerimientos de ancho de banda necesarios para la red y la topología en estrella. Como la red contará con la combinación de velocidades de 10, 100 y 1000 Mbps, los dispositivos con las velocidades más altas deberán ser compatibles con los que operen a las velocidades más bajas.

3.2.2.1.1 Dispositivos Terminales

Los dispositivos terminales que interactuarán en la red son: estaciones de trabajo del tipo portátil y de escritorio, terminales ligeros *Thin-Client*, teléfonos IP, y adaptadores de teléfonos analógicos ATAs, para conectar dispositivos fax, teléfonos analógicos y teléfonos inalámbricos DECT (*Digital Enhanced Cordless Telecommunication*).

Las estaciones de trabajo y terminales ligeros se conectarán directo a puntos de red de datos con cables *patch cord* UTP categoría 6, de 3 metros máximo. Todas las estaciones de trabajo tienen NIC *Fast Ethernet* integradas con velocidades de 10/100 Mbps. Las características de *hardware* y *software* dependen directamente de las aplicaciones que se vayan a utilizar. Las estaciones de trabajo y terminales ligeros presentan como sistemas operativos: *Windows XP*, *Windows Vista* y *Windows 7*.

Los teléfonos IP se conectarán directamente a los puntos de red etiquetados como puntos de voz, con cables *patch cord* UTP categoría 6 y que no superen los 3 metros. Todos los teléfonos tendrán NIC *Fast Ethernet* con velocidades de 10/100 Mbps. En Quito se cuenta con un teléfono analógico que debe ser integrado al sistema telefónico IP, al igual que un teléfono inalámbrico DECT de Guayaquil. Estos dispositivos más las máquinas de fax se conectarán a puntos de voz mediante cables con conectores RJ-11, y contarán con ATAs para que interactúen con el sistema telefónico IP. Las características específicas de cada terminal telefónico dependerán de qué tipo son y de la necesidad del usuario. Éstas se discutirán más adelante.

3.2.2.1.2 Equipos de Conectividad

Los equipos de conectividad que estarán presentes en este diseño de red son: *switches* y *gateways* de voz (que pueden ser implementados también en *routers*) como parte de la red corporativa de Alianza, *routers* y *modems* como parte de la red del proveedor de servicios.

Los *switches* se dividirán en *switches* de acceso, *switches* de distribución y *switches* de núcleo, estarán ubicados dentro del cuarto de equipos o del cuarto de telecomunicaciones del área que brinde el servicio, manejarán tecnología *Fast Ethernet* y *Gigabit Ethernet* y se conectarán siguiendo el modelo jerárquico propuesto. A los *switches* se conectarán los dispositivos terminales de usuario para que accedan a los servicios.

Los *gateways* de voz harán las conversiones de protocolos requeridas y se utilizarán para la conexión de la central o servidor de Telefonía IP con la PSTN. Contarán con puertos RJ-45 presentes en NICs *Fast Ethernet*.

3.2.2.1.3 Servidores

Se mantendrán los mismos servidores, salvo algunas excepciones que se redimensionarán posteriormente. Los servidores se manejarán exclusivamente dentro de los cuartos de equipos ubicados en el Departamento de Sistemas, presentarán características de *hardware* dependiendo de los servicios y aplicaciones que brinden en la red. Manejarán sistemas operativos *Windows Server* en las versiones 2003 y 2008, se mantendrán las tarjetas de red actuales, con tecnologías *Fast Ethernet* y *Gigabit Ethernet*. Los servidores se conectarán al *switch* de *core* para brindar los servicios a los usuarios utilizando cables *patch cord* UTP categoría 6.

3.2.2.2 Conectividad

3.2.2.2.1 Capa de Acceso ^[2]

En esta capa se conectarán los dispositivos terminales a los *switches* de acceso, con velocidades de 10/100 Mbps, lo cual es suficiente dado que por usuario se necesitará un ancho de banda de aproximadamente 1 Mbps. Para que los *switches* de acceso sean compatibles con la mayoría de dispositivos terminales, sin importar la velocidad a la que operen (10 ó 100 Mbps), o si requieren cable directo o cruzado, sus puertos RJ-45 deben tener las características *Auto-sense* y *MDI/MDI-X*.

Los terminales telefónicos se conectarán a puertos del *switch* que tengan la tecnología PoE (*Power over Ethernet*), estándar IEEE 802.3af, para suministrar energía eléctrica a los teléfonos IP a través del cable UTP.

Los *switches* de acceso utilizarán el método de conmutación *Fragment Free*, el cual asegura que las tramas transmitidas sean, al menos, del tamaño mínimo permitido con una baja latencia de procesamiento; con ello se favorecerá trabajar con aplicaciones de voz, por ser sensible a la excesiva pérdida de paquetes y a las constantes retransmisiones que implican los retardos. En su ausencia, se utilizará el método *Store & Forward* que procesa toda la trama, con una latencia mayor, pero de forma más confiable.

Los *switches* de acceso se conectarán con enlaces *Gigabit Ethernet* a la capa distribución. Utilizarán 2 puertos *uplink* de 10/100/1000 Mbps con conectores RJ-45.

3.2.2.2.2 *Capa de Distribución*

En la capa de distribución se necesitarán equipos de conectividad de alta capacidad para el soporte del tráfico de voz y datos. Se manejará una topología en estrella, la misma que permitirá conectar todos los *switches* de acceso a los de distribución. Las funciones de la capa de distribución de Quito se implementarán en su totalidad, debido al número de usuarios y por la cantidad de transacciones que se realizan hacia los servidores. Para Guayaquil se unificarán las funciones más importantes de las capas de distribución y núcleo en un solo

switch, para abaratar costos y porque los servicios se concentrarán mayormente en Quito.

Dado que la capa de distribución es la responsable de redirigir el tráfico desde el origen hasta el destino, es el lugar apropiado para implementar el control y filtrado de paquetes. El mecanismo más común de filtrado es con Listas de Control de Acceso o ACLs.

La capa de distribución está encargada de manejar la carga de tráfico, producto de todos los usuarios y servidores, así que la tasa de envío de paquetes debe ser superior a la de la capa acceso. Más adelante se muestra el dimensionamiento de los paquetes por segundo que deberán ser capaces de transmitir los *switches*. Los *switches* de distribución se conectarán con enlaces *Gigabit Ethernet* a la capa de núcleo con dos puertos *uplink* de 10/100/1000 Mbps y conectores RJ-45.

Para Quito se propone la utilización de dos *switches* de distribución con enlaces redundantes hacia las capas de acceso y núcleo, por motivos de disponibilidad y balanceo de carga. El primer *switch* de distribución mantendrá enlaces primarios con 3 de los 5 *switches* de acceso y el segundo, con los dos restantes. Los enlaces de respaldo se distribuirán de forma inversa. Estos enlaces secundarios operarán únicamente cuando se suscite algún inconveniente con los enlaces primarios. En la figura 3.7 se muestran estas conexiones.

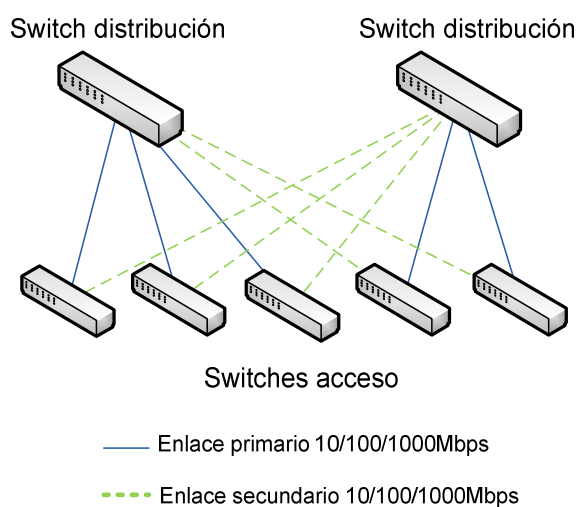


Figura 3.7 Conexión entre las capas distribución y acceso

3.2.2.2.3 Capa de Núcleo ^{[32][33][34]}

En el caso de la red corporativa de Alianza de Seguros se tiene una capa de núcleo para la red LAN Quito y otra para la red Guayaquil; ambas interconectadas mediante el enlace WAN. Aquí se encontrarán los servidores de la empresa, los *switches* de *core*, los *gateways* de voz, los *routers* y módems de acceso WAN. Estos últimos serán responsabilidad de la empresa proveedora de servicios de transporte de datos, en concordancia a los acuerdos de nivel de servicio.

Los servidores se conectarán a la capa núcleo mediante enlaces *Gigabit Ethernet*, para evitar “cuellos de botella” que podrían ocasionar congestión en la red. Además, debido a la necesidad de que el núcleo reenvíe los paquetes lo más rápido posible, el *switch* de esta capa deberá tener la tasa de envío de paquetes más alta en comparación con los *switches* de las capas inferiores.

En el núcleo de Quito cada *switch* de distribución se conectará al *switch* de núcleo con dos enlaces redundantes. Se conectarán mediante agregación de enlaces para disponer un ancho de banda de 2 Gbps. En caso de falla de un enlace redundante se transmitiría con un ancho de banda de 1 Gbps hasta habilitar el enlace que falló. Los *switches* de distribución se conectarán entre sí mediante un único enlace de 10/100/1000 Mbps, desactivado hasta el momento en que se caiga algún enlace primario que conecta distribución con núcleo. Para evitar los posibles lazos que se puedan presentar por la redundancia, se necesita el protocolo STP (*Spanning Tree Protocol*, IEEE 802.1D) en cada *switch*. En la figura 3.8 se muestran las conexiones entre capa núcleo y distribución.

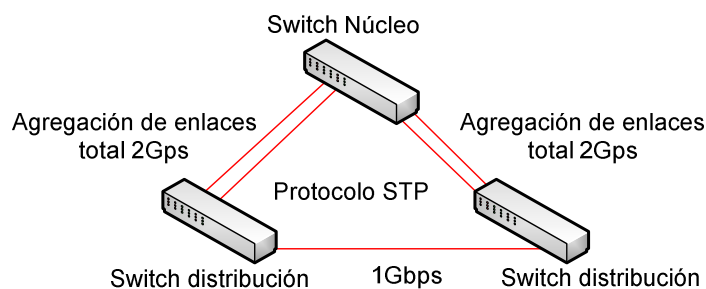


Figura 3.8 Conexiones entre las capas núcleo y distribución

Para la ciudad de Guayaquil se propone que los *switches* de acceso se conecten directamente al único *switch* de núcleo con enlaces redundantes 10/100/1000 Mbps y puerto RJ-45.

Todos los servicios de red empresariales dependen del núcleo de la red, por lo que se requerirá que los *switches* de esta capa tengan un tiempo promedio entre fallas, MTBF (*Mean Time Between Failures*) mayor o igual al doble del tiempo contemplado para el diseño, es decir, 10 años.

En el *switch* de núcleo se realizará la interconexión entre VLANs (estándar IEEE 802.1Q). Cada VLAN corresponde a un dominio de *broadcast* diferente, por lo que para su interconexión se requiere de conectividad a nivel de capa 3 con direcciones IP. Por lo tanto, se requiere que el *switch* pueda realizar enrutamiento estático o dinámico. El enrutamiento dinámico se preferirá con RIPv2 (RFC 2453), para el soporte de *subnetting*.

El crecimiento de la red y futuras expansiones requieren el soporte de fibra óptica, ya que la mayoría de *carriers* están migrando a esta tecnología por su capacidad. Se considerará la utilización de puertos de fibra SFP-GBIC.

3.2.2.3 Diseño Lógico de la Red

En el diseño lógico de la red se definirá el direccionamiento IP para todas las sucursales, las VLANs a crearse y el enrutamiento entre ellas. Con la integración de la Telefonía IP se definirán también el plan de numeración telefónico, categorización de usuarios y los grupos de usuarios para llamadas telefónicas.

Alianza de Seguros cuenta con agencias en Quito, Guayaquil, Cuenca, Machala, Sto. Domingo, Manta y Milagro. Aunque este proyecto es sólo para las dos primeras localidades, se plantea el diseño lógico para todas las sucursales por motivos de administración, unificación y consistencia de toda la red.

3.2.2.3.1 *Direccionamiento IP*

Para el direccionamiento IP se tomó como referencia el número de usuarios y la antigua distribución de direcciones IP. Se utilizará la dirección IP privada clase C 192.168.0.0 con máscara de red 255.255.0.0. Esta red se dividirá en subredes, una por cada sucursal. Para diferenciar el tráfico de voz y datos, las subredes de Quito y Guayaquil se subdividirán a su vez en dos. La capa núcleo será la encargada de su interconexión.

En la tabla 3.6 se detalla la división de subredes divididas sus respectivas máscaras de subred y el rango de direcciones IP válidas.

Ciudad	Subred	1era dirección	Última dirección	Dirección de Broadcast	Máscara de subred
Quito	192.168.1.0	192.168.1.1	192.168.1.126	192.168.1.127	255.255.255.128
UIOVOZ	192.168.1.128	192.168.1.129	192.168.1.254	192.168.1.255	255.255.255.128
Cuenca	192.168.2.0	192.168.2.1	192.168.2.254	192.168.2.255	255.255.255.0
Guayaquil (centro)	192.168.3.0	192.168.3.1	192.168.3.126	192.168.3.127	255.255.255.128
GYEVOZ	192.168.3.128	192.168.3.129	192.168.3.254	192.168.3.255	255.255.255.128
Manta	192.168.4.0	192.168.4.1	192.168.4.254	192.168.4.255	255.255.255.0
Sto. Domingo	192.168.5.0	192.168.5.1	192.168.5.254	192.168.5.255	255.255.255.0
Machala	192.168.6.0	192.168.6.1	192.168.6.254	192.168.6.255	255.255.255.0
Tecno-Alianza	192.168.7.0	192.168.7.1	192.168.7.254	192.168.7.255	255.255.255.0
Guayaquil (Kennedy)	192.168.8.0	192.168.8.1	192.168.8.254	192.168.8.255	255.255.255.0
Milagro	192.168.9.0	192.168.9.1	192.168.9.254	192.168.9.255	255.255.255.0

Tabla 3.6 *Direccionamiento IP de subredes*

Las estaciones de trabajo y los teléfonos IP contarán con una configuración estática de direcciones IP, que facilita el control de estos terminales.

Se contará con una subred exclusiva de administración a la que sólo tenga acceso personal técnico. La subred de administración tendrá la dirección 192.168.99.0/28, a la que se aplicará una VLAN independiente.

3.2.2.3.2 VLANs

Se plantea la creación de VLANs para mejorar la organización, el rendimiento, la seguridad y la calidad de servicio en la red. La red estará dividida en tres VLANs: datos, voz y administración, que deberán ser configuradas en todos los *switches* de la red. En la tabla 3.7 se muestran las VLANs creadas para las sucursales.

Ciudad	Subred	Etiqueta	VLAN ID
Quito	192.168.1.0	SEG_DATOS	VLAN10
UIOVOZ	192.168.1.128	SEG_VOZ	VLAN20
Cuenca	192.168.2.0	SEG_DATOS	VLAN10
Guayaquil	192.168.3.0	SEG_DATOS	VLAN10
GYEVOZ	192.168.3.128	SEG_VOZ	VLAN20
Manta	192.168.4.0	SEG_DATOS	VLAN10
Sto. Domingo	192.168.5.0	SEG_DATOS	VLAN10
Machala	192.168.6.0	SEG_DATOS	VLAN10
Tecno-Alianza	192.168.7.0	SEG_DATOS	VLAN10
Guayaquil (Ken)	192.168.8.0	SEG_DATOS	VLAN10
Milagro	192.168.9.0	SEG_DATOS	VLAN10
Administración	192.168.99.0	SEG_ALIANZA	VLAN99

Tabla 3.7 Segmentación de VLANs

Los puertos de los *switches* de acceso se dividirán en puertos de voz y datos para definir las VLANs respectivas. En los puertos de voz se activará PoE y se conectarán los teléfonos IP. En los puertos de datos se conectarán los computadores. En caso de que se utilice el *switch* interno del teléfono IP para la conexión de una computadora, éste será el encargado de la etiquetación. Todo el tráfico no etiquetado que vaya al *switch* será ubicado en la VLAN de datos.

3.2.2.3.3 Enrutamiento entre VLANs

La interconexión entre VLANs se realizará en la capa de núcleo. Los *switches* de distribución pasarán las VLANs a otros *switches* a través de puertos en modo

trunk. En la figura 3.9 se muestra el diagrama lógico de la configuración de VLANs.

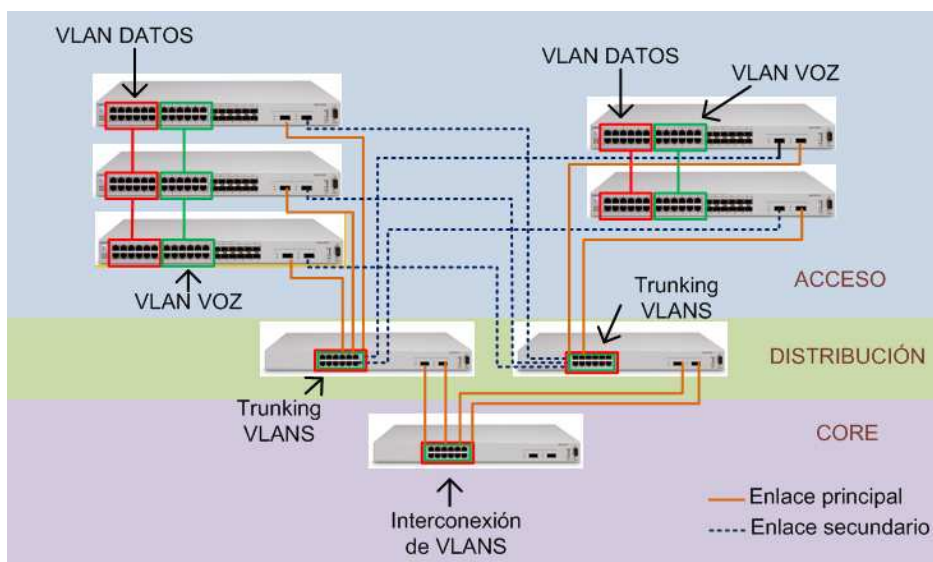


Figura 3.9 Diagrama lógico del funcionamiento de VLANs

3.2.2.3.4 Plan de Numeración

El plan de numeración del sistema telefónico dependerá del número de usuarios que se tendrán para cada sucursal. Para la numeración de las extensiones en las diferentes localidades de la empresa se ha previsto utilizar un dígito para el prefijo de sitio y dos dígitos para identificación de la extensión, con lo que se tienen 3 dígitos de numeración. En la tabla 3.8 se detalla el plan de numeración.

Ciudad	Prefijo de sitio	Número inicial	Número Final
Quito	1	100	199
Cuenca	2	200	299
Guayaquil	3	300	399
Manta	4	400	499
Sto. Domingo	5	500	599
Machala	6	600	699
Guayaquil (Ken)	7	700	799
Milagro	8	800	899

Tabla 3.8 Plan de numeración propuesto para Telefonía IP

El plan de numeración también incluye las sucursales que mantendrán sus sistemas de Telefonía tradicional. Se las incluye por cuestiones de comodidad y para mantener un sistema de numeración homogéneo.

3.2.2.3.5 Categorización de Usuarios

El perfil de usuario telefónico se basará en dos aspectos fundamentales: tipo de usuario y tipo de acceso al servicio telefónico.

Los tipos de usuarios se definieron en el capítulo 2, donde se clasificó al usuario dependiendo de su naturaleza y las actividades que desempeña. En la clasificación se establecen los usuarios administrativos, operativos y de mantenimiento. Para ellos se definirá el tipo de acceso requerido.

El tipo de acceso al servicio telefónico se refiere al tipo de llamadas que el usuario podrá realizar. Las llamadas pueden ser: internacionales, nacionales, regionales, locales, celulares, internos, de emergencia y números locales especiales. Los números locales especiales son aquellos números telefónicos que representaría la realización de una llamada local hacia una empresa en especial para una emergencia. Dentro de este esquema entra el guardia de seguridad que requerirá realizar una llamada telefónica a la empresa de seguridad para la que trabaja y reportar algún incidente que se suscite. En la tabla 3.9 se realiza la categorización o perfil de usuario para la empresa Alianza de Seguros.

Tipo	Usuarios	Nacional	Internac.	Reg.	Local	Interno	Cel.	Números emergencia
Administrativo	Gerencia General	✓	✓	✓	✓	✓	✓	✓
	Gerencias de departamentos	✓	x	✓	✓	✓	✓	✓
Operativo	Ejecutivos, técnicos y productores de seguros	x	x	✓	✓	✓	x	✓
Mantenimiento	Limpieza y conserje	x	x	x	✓	✓	x	✓
	Guardia		x	x	x	✓	x	✓

Tabla 3.9 Perfil de usuarios telefónicos de Alianza de Seguros

Todos los perfiles de usuarios tendrán configurados el tiempo de duración de una llamada, para así evitar gastos innecesarios de recursos en actividades que no representen productividad para la empresa. La duración máxima de una llamada será de 5 minutos para las labores cotidianas de los usuarios.

3.2.2.3.6 Grupos de usuarios telefónicos ^[10]

En Telefonía IP se pueden definir métodos para redirigir las llamadas a un grupo específico de extensiones, según diversos criterios como: el tipo de usuario, tipo u origen de la llamada, etc. Estos grupos se denominan grupos de caza (*hunt groups*). Los grupos de caza se pueden definir para varias aplicaciones como: parqueo y captura de llamadas (*call park/call pickup*), encuéntrame/sígueme (*find-me/follow-me*), agentes de *call center*, entre otras.

Los grupos de usuarios telefónicos se dividirán por departamentos dentro de la empresa, así por ejemplo, si una llamada telefónica va dirigida a un agente de cuenta en el Departamento de Siniestros y éste se encuentra con la línea ocupada, esta llamada será redireccionada automáticamente a otro agente de cuenta para que concrete el pedido. También puede ser redirigida a otra persona del mismo departamento que se encuentre dentro del grupo de usuarios. La división en departamentos servirá para brindar ayuda e información al cliente o emisor de la llamada ya que se podrán comunicar con otra persona que conoce sobre el tema o actividad específicos. A continuación se enlistan los grupos de usuarios que se crearán:

- Caja
- Cobranzas
- Emisión
- Siniestros
- Producción
- Sistemas
- Recursos Humanos
- Contabilidad

El resto de departamentos no se consideran dentro del esquema de grupos de usuarios telefónicos ya que son departamentos pequeños, con uno o dos usuarios como máximo. Es importante mencionar que los gerentes no entrarán en el esquema de grupos de llamadas, pero se configurará el reenvío de llamadas hacia sus asistentes cuando no se encuentren disponibles los gerentes.

3.2.3 SERVICIOS Y APLICACIONES

En el capítulo anterior se han identificado los servicios que “corren” en la red de Alianza de Seguros, los cuales se listan a continuación:

- Base de datos
- Antivirus
- Aplicaciones
- Escritorio remoto
- Correo Electrónico
- Compartición de archivos
- Acceso WEB
- DNS
- DHCP
- *Firewall*
- Directorio
- Video-vigilancia

Algunos de estos servicios han sido desplegados de manera no planificada o desordenada y necesitan ser reorganizados. En otros casos, se necesita redimensionarlos, mejorar su funcionamiento e integración dentro de la red, así mejorar las aplicaciones con las que se accede a ellos.

A estos servicios se añadirán los de Telefonía IP, como llamadas, conferencias, mensajería unificada, entre otros.

Todos los servicios mencionados son para uso interno de la empresa. Por el momento no existen planes inmediatos de prestar servicios para usuarios externos.

Los requerimientos de *hardware* o *software* adicionales para cada servicio se especifican en la sección de dimensionamiento.

3.2.3.1 Reorganización de los Servicios y Aplicaciones Existentes

La red corporativa, mediante el enlace WAN, servirá para que los servicios ubicados físicamente en Quito o Guayaquil, puedan ser accedidos por los usuarios desde cualquiera de las sucursales indistintamente. Sin embargo, es conveniente mantener algunos servicios en el entorno local ya sea por disponibilidad, porque la información es pertinente sólo para una sucursal en particular, o para descongestionar el enlace WAN. En la tabla 3.10 se muestra el detalle de dónde se ubicarán los servicios, cuál será su ámbito y una breve descripción adicional. Los servicios de Telefonía IP se tratarán en el apartado siguiente; el acceso WEB estará dentro el dimensionamiento del enlace WAN y el de *firewall* en la sección de Seguridad.

En las siguientes secciones se detallan los cambios que se proponen para mejorar el funcionamiento e integración de los servicios y aplicaciones de la red. Los servicios no mencionados seguirán operando de la misma forma que lo han venido haciendo.

3.2.3.1.1 Base de Datos ^{[6][35]}

El servicio de bases de datos se mantendrá intacto en su servidor, ya que no se han encontrado problemas con el mismo. Actualmente los usuarios acceden a este servicio a través de una terminal con el protocolo TELNET. En este caso se sugerirá el uso de clientes ya sea WEB vía HTTPS, o mediante conectores ODBC (*Open DataBase Connectivity*) con seguridad para el acceso a la base datos DB2,

dados los riesgos de seguridad que implican los mensajes en texto plano de TELNET.

3.2.3.1.2 Antivirus

Para optimizar el uso del ancho de banda de la WAN y del acceso a Internet, se cambiará la programación de las actualizaciones fuera del horario de oficina, es decir, pasadas las 18:00 de lunes a viernes o a su vez en fines de semana, ya que en el análisis de tráfico del capítulo 2 se comprobó que estos horarios son los menos congestionados para los enlaces.

Servicio	Ciudad	Ámbito / Característica
Base de datos	Quito	Red corporativa. Acceso mediante <i>software</i> cliente de usuario.
Antivirus	Quito	Red corporativa. Acceso con agentes distribuidos en sucursales.
Aplicaciones	Quito	Local. Se pretende ampliar su uso desde clientes remotos.
Escritorio remoto	Quito Guayaquil	Red corporativa. Los Administradores de la red pueden acceder desde cualquier sucursal a cualquier equipo.
Correo Electrónico	Quito	Red corporativa. Acceso desde cualquier sucursal.
Compartición de archivos	Quito Guayaquil	Local. Se almacenarán archivos de índole local: documentos, imágenes, presentaciones, etc.
Acceso WEB	Quito	Red corporativa. El acceso WEB o acceso a Internet en general, se contratará y controlará desde la ciudad de Quito.
DNS	Quito	Red corporativa. El servicio de consulta de nombres de dominio se brindará desde la ciudad de Quito, donde residirá el acceso a la Internet.
DHCP	Quito Guayaquil	Local. Las direcciones se asignarán dinámicamente en el ambiente local.
Directorio	Quito	Red corporativa. Se integrarán los servicios principales para proveer un servicio de directorio único y consolidado.
Video-vigilancia	Guayaquil	Red corporativa. El servidor y las cámaras de vigilancia se encuentran únicamente en Guayaquil, pero pueden ser accedidas desde otras sucursales.

Tabla 3.10 Ubicación y ámbito de los servicios existentes en la red corporativa

3.2.3.1.3 Correo Electrónico ^{[7][36]-[39]}

El servicio de correo electrónico se separará del servidor Kypus, que funge de *firewall*, por los riesgos de seguridad que esto implica. Este servidor al estar

expuesto a la Internet y otras redes, puede ser víctima de ataques, y si cae o es “hackeado”, la información privada de los correos puede verse comprometida.

Se propone que la plataforma para el nuevo servidor de correo electrónico sea basada en Linux *kernel* 2.6 o superior con un MTA (*Mail Transport Agent*) *Qmail* 1.03 o superior, por la compatibilidad con el sistema de correo electrónico anterior que también usa Linux y que usa como MTA a *Sendmail*.

Qmail se considera un MTA más seguro y simple que *Sendmail*. Soporta los mismos protocolos: SMTP (*Simple Mail Transfer Protocol*) para transporte de mails entre MTAs, o IMAP4 (*Internet Message Access Protocol v4*) y POP3 (*Post Office Protocol v3*) para que el MUA (*Mail User Agent*), en este caso *MS Outlook*, pueda recuperar el correo electrónico del servidor. Finalmente, existe la suficiente documentación sobre el proceso de migración del servicio de correo electrónico de *Sendmail* a *Qmail*. De esta manera no se afecta la forma como los usuarios han venido trabajando con este servicio.

El cliente de correo *MS Outlook* será configurado por defecto con el protocolo IMAP4 para el acceso a la bandeja de correo. Frente a POP3, IMAP4 tiene la ventaja de mantener los correos en el servidor, lo que posibilita su revisión desde múltiples dispositivos terminales.

3.2.3.1.4 *Compartición de archivos*

En Guayaquil se agregará el servicio de compartición de archivos. Éste funcionará de forma similar al de Quito y almacenará todo tipo de documentos que la sucursal requiera. Estará basado en una plataforma *Microsoft Windows Server* para que los usuarios puedan acceder al servicio con sus computadores, también basados en *Microsoft Windows*, al igual que en Quito.

3.2.3.1.5 DHCP, DNS, y Directorio ^{[8][9]}

El servicio de DHCP se prestará individualmente en cada sucursal y permitirá a equipos temporales acceder a la red de forma rápida.

El servicio DNS será configurado en la sucursal de Quito que es donde se controla el acceso a Internet, usado básicamente para navegación WEB y correo electrónico.

El servicio de directorio se considera básico dentro de cualquier red ya que permite administrar correctamente a usuarios y recursos a través de sus credenciales. En la red de Alianza se establecerá un directorio unificado a través de las dos plataformas que manejará, *Microsoft Windows* y *Linux*. El producto de *Microsoft* ya desplegado en la red, *Active Directory*, se considera uno de los más robustos del mercado, por lo que se lo tomará como controlador de directorio primario. Para *Linux* se contará con el controlador de directorio *OpenLDAP* y se lo integrará con *Active Directory* para que se utilicen las mismas credenciales de usuario en los servicios que necesitan autenticación. Esta integración es posible ya que los dos controladores de directorio, en sus últimas versiones, están basados en el estándar *LDAPv3 (Lightweight Directory Access Protocol* versión 3). Este protocolo también se requerirá para integrar los servicios de Telefonía IP con el directorio.

3.2.3.2 Servicio de Telefonía IP, Colaboración y Comunicaciones Unificadas

Con la inclusión de los servicios de voz dentro de la red corporativa se proveen también una serie de servicios adicionales que, integrados, apuntan a agilizar la productividad empresarial. La mensajería unificada, vista como la integración de mensajes de múltiples fuentes en un único buzón de correo; la integración de servicios como el directorio y la base de datos; la presencia y la mensajería instantánea, como comunicaciones en tiempo real basadas en el estatus de actividad y locación del usuario, son las principales prestaciones que se incluirán dentro de este capítulo y se revisarán en esta sección.

A pesar de que el video y la movilidad están fuera del alcance de este proyecto, se mencionarán los lineamientos básicos de soporte para estas características, como un acercamiento de esta red al concepto de comunicaciones unificadas.

Todas estas funciones se pueden implementar independientemente del protocolo de señalización, el cual se analizará y seleccionará en la sección de soluciones de Telefonía IP.

3.2.3.2.1 Descripción del servicio de Telefonía IP

El esquema de Telefonía IP que se plantea tiene muchas similitudes con el sistema telefónico tradicional: un equipo centralizado para el control de las llamadas, terminales telefónicos, y un cableado que permite conectar todos los dispositivos al equipo de control. La diferencia más importante es que todos estos elementos pasan a compartir y formar parte de la infraestructura de la red de datos. Así, la Telefonía se convierte en uno más de sus servicios.

El servidor de Telefonía IP se encargará fundamentalmente de la señalización para dirigir las llamadas desde su origen hacia su destino, sea en la red local, en otra sucursal atravesando la WAN, o en la PSTN. Dentro de la red corporativa todas las comunicaciones se harán vía IP, y la voz codificada con los códecs G.711, G.722 o G.729 se encapsularán en RTP como medio de transporte en tiempo real. Sin embargo, para usar los servicios de la PSTN se deberán hacer la conversiones digitales o analógicas (con tonos DTMF) respectivas. Se contará con un *media gateway* para las traducciones, ya sea de los códecs de voz, faxes o cualquier otro tipo de medio que se necesite, para interactuar con los servicios de la PSTN. El servidor y el *media gateway* pueden ser equipos independientes o ser integrados en un único *hardware*. El servidor será también el encargado de llevar el registro y control sobre el uso del sistema telefónico, así como de almacenar mensajes de voz y faxes, o a su vez de reenviarlos al servidor de correo electrónico para que sus destinatarios revisen su contenido posteriormente. Las funciones de mensajería instantánea y presencia se controlarán preferentemente desde este equipo.

Alianza de Seguros se puede catalogar como una empresa mediana, dado el número de usuarios que asciende a la centena. En Quito se concentran cerca de 52 usuarios y en Guayaquil, 31. Dada esta distribución, en Quito se establecerá el servidor de Telefonía principal que controlará todos los servicios relacionados con llamadas y mensajería unificada, así como la integración con otros servicios de la red. En Quito y Guayaquil se tendrán *media gateways* capaces de comunicarse y ser controlados por el servidor de Telefonía principal a través de la red corporativa. También proveerán el acceso a la PSTN de manera local. Las dos sucursales se comunicarán mediante el enlace WAN.

Del lado del usuario se encontrarán los teléfonos IP, teléfonos analógicos fuera del alcance del cableado estructurado, y las máquinas analógicas de fax. Mediante el panel visual de los teléfonos más las teclas programables y de navegación, los usuarios podrán realizar y recibir llamadas, participar en conferencias, revisar su correo de voz, etc. También existe la posibilidad de usar el computador para acceder a los servicios telefónicos a través de productos de *software* tales como *softphones*. Si un usuario no se encuentra en condiciones de contestar una llamada en particular, será el servidor el que decida qué acción tomar a través de las funciones de control básicas y avanzadas. La figura 3.10 bosqueja los elementos del servicio de Telefonía IP.

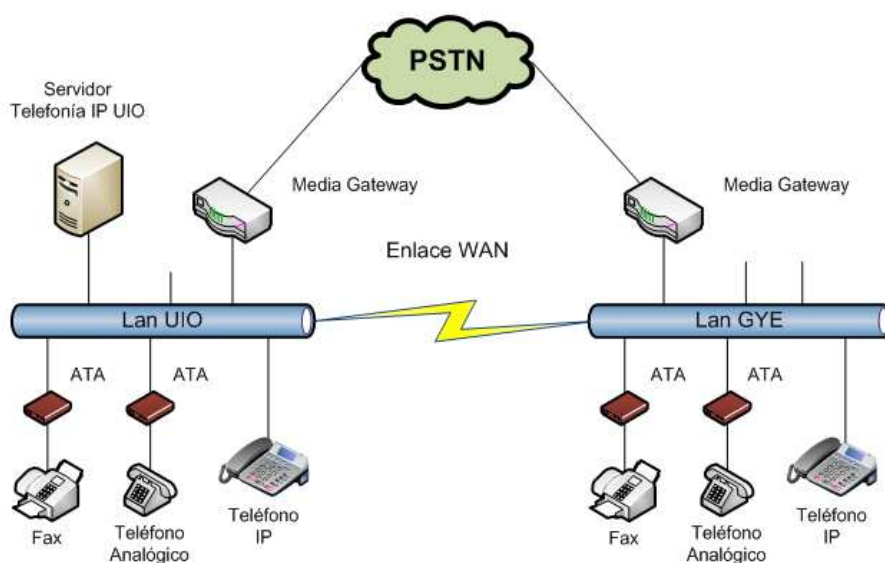


Figura 3.10 Elementos de Telefonía IP dentro de la red corporativa

Para que los dispositivos analógicos formen parte del sistema telefónico IP, se contará con el uso de ATAs. Estos dispositivos son *gateways* que permiten la conversión de los protocolos usados en la red IP a señales analógicas para teléfonos y faxes, entre otros.

Una ventaja del uso de *gateways* y ATAs independientes, es la disminución de la carga de procesamiento digital en el servidor de Telefonía IP.

3.2.3.2.2 *Prestaciones básicas de Telefonía relacionadas con las llamadas*^{[10]-[13]}

Las prestaciones que deberá soportar el nuevo sistema telefónico IP en relación al comportamiento, control y uso de las llamadas se muestran en la tabla 3.11.

3.2.3.2.3 *Mensajería Unificada*^{[10][14]}

El servidor de Telefonía es el destino inmediato de los mensajes de voz, intencionados o fruto de llamadas no atendidas. Integra a su infraestructura las líneas externas de fax y a los facsímiles analógicos; de esta manera administra tanto mensajes de voz como los faxes, para almacenarlos o distribuirlos a diferentes destinos. Gracias a la incorporación de los protocolos estándar de correo electrónico como SMTP o IMAP, el servidor de Telefonía IP estará en la capacidad de remitir los mensajes al servidor de correo electrónico propio de la empresa. Así queda consolidado el buzón único de correo que sustenta la mensajería unificada. Los mensajes de voz se almacenarán con el formato WAV (*WAVEform audio format*) comprimido u otras opciones que hagan uso eficiente del espacio en disco.

La integración del fax a la red IP mediante el *media gateway* puede realizarse de 3 formas distintas, denominadas como:

- ***Passthrough***: El más simple de todos, actúa como una llamada de voz común. El *gateway* recibe una forma de onda analógica desde la línea de

fax, la codifica con G.711 comúnmente, y la encapsula con RTP para enviarla a la red IP.

Prestación	Descripción
Operadora automática	Aplicación telefónica que provee sugerencias y saludos interactivos para las llamadas entrantes de una PBX o servidor, de tal manera que las llamadas pueden ser enrutadas sin la intervención de una persona como recepcionista.
Ruta del de menor costo	Función que permite enrutar las llamadas a través de la línea del menor costo en base a algoritmos programables.
Servicios de emergencia 911	De existir este servicio en el área, la llamada es enrutada a él de inmediato. Una característica importante es la ubicación automática del origen de la llamada.
Búsqueda en directorio	Mediante el teléfono se puede acceder al directorio telefónico del servidor para buscar contactos por extensión o por nombre.
Conferencia: modo Ad hoc modo Meet-me	Permite a más de dos usuarios mantener una conversación telefónica. Modo Ad hoc: el usuario que inicia la conferencia decide a qué otros usuarios añade. Modo Meet-me: los usuarios pueden adherirse a la conferencia voluntariamente
Desvío de llamadas	Las llamadas marcadas con un número son re-enrutadas a otro número.
Transferencia de llamadas	Una llamada en progreso puede ser transferida a otra extensión y continuar en ella.
Parqueo y captura de llamadas	Permite poner a una llamada en espera en extensiones “virtuales” hasta que se encuentre al destinatario. Cuando el destinatario está listo para contestar, marca la extensión virtual y entonces captura la llamada.
Llamada en espera	Una llamada que está en proceso puede ser puesta en espera sin colgar, para contestar o realizar una segunda llamada. La llamada inicial puede ser recuperada luego de que se finalice la segunda llamada.
Encuéntrame/Sígueme	Forma de desvío de llamada que “busca” a un usuario en diferentes terminales telefónicos en un orden preestablecido.
Alerta de límite de tiempo para llamadas.	Alerta ya sea visual o sonora que indica que se ha alcanzado el tiempo máximo de la llamada entrante o saliente pre programado.
Identificador de llamadas	Función que permite visualizar en el teléfono la identificación de quien realiza la llamada entrante.
Historial de llamadas	Función que permite revisar las extensiones marcadas y el tiempo de duración de la llamada en el teléfono.
Música en espera	Función que permite tocar música cuando una llamada está en espera.
Indicador de llamadas y mensajes en espera	Indicador visual que se activa en el teléfono cuando existe un mensaje o una llamada entrante en espera.
Remarcado	Función que permite marcar el último número usado.
Marcado rápido	Acceso a los números más usados a través de teclas pre programadas.
No molestar	Cuando se tiene activada esta función en el teléfono, antes de que la llamada llegue al destino, se la reenvía a otra extensión o al buzón de mensajes.
Devolución de llamada automática	Si una extensión que está ocupada recibe una llamada, al liberarse el teléfono marca automáticamente el número de la última llamada entrante.

Tabla 3.11 *Prestaciones básicas del servicio telefónico*

- **Fax Relay (T.38⁷):** El gateway debe demodular la señal analógica con el protocolo T.30 para recuperar la señal binaria de datos contenida. Una vez obtenidos los bits, éstos se transportan por la red IP con el protocolo T.38.

⁷ T.38, T.37 y T.30 son estándares de la ITU-T que definen los métodos de transporte para fax dentro de una red IP.

Este protocolo contenido en un ATA, se encarga de volver a modular la señal binaria para que el facsímil la entienda.

- **Store & Forward (T.37):** En este modo el *gateway* decodifica la señal analógica con el protocolo T.30 y envía el fax como correo electrónico a través de SMTP al servidor de correo para almacenarlo. Para el proceso inverso, el correo viaja hasta el *gateway* donde está conectado el facsímil y se transforma a fax.

De los tres modos de integración de fax descritos se concluye que con el soporte de los protocolos T.38 y T.30 en el *media gateway* más el protocolo SMTP en el servidor, se puede proveer de fax en tiempo real y fax-a-correo para la empresa. Se debe inferir que en el esquema de fax-a-correo, éste puede ser impreso luego de su recepción, por lo que la máquina facsímil carece de utilidad. Por compatibilidad entre aplicaciones, los formatos preferidos para almacenar el fax como correo electrónico serán PDF (*Portable Document Format*), PNG (*Portable Network Graphics*) y TIFF (*Tagged Image File Format*).

Otra opción importante de mensajería unificada es la integración con *MS Outlook*. Una vez integrado el servidor de correo con el servicio telefónico, el cliente de correo *MS Outlook* puede recuperar faxes y mensajes de voz en su bandeja. A más de esto, se pueden realizar llamadas directamente desde la lista de contactos de *MS Outlook* gracias a la opción click-para-marcar.

3.2.3.2.4 Integración con otros servicios de red

Además de los servicios descritos, existen otras posibilidades de integración que se describen a continuación:

- **Con el directorio.** Para evitar la disgregación y replicación de información en las cuentas de usuario en un ambiente multi-servicios, la plataforma de Telefonía IP manejará el directorio telefónico mediante el protocolo LDAPv3, que permite unificarlo con el servicio de directorio de la compañía.

- **Con la base de datos.** El servicio de base de datos es una rica fuente de información con la cual Alianza puede añadir mucho valor a sus servicios, tanto a nivel interno, como con sus clientes. La integración con el servicio de base de datos se da mediante conectores estándar como los ODBC y se pueden implementar características muy avanzadas como la respuesta de voz interactiva conocida como IVR, la conversión voz/texto o *call centers*. Para su implementación, estas características requieren un análisis más riguroso y detallado; y aunque están fuera del alcance de este proyecto, se han sentado las bases para su soporte.

3.2.3.2.5 *Servicios opcionales y futuros de comunicaciones unificadas* ^{[15][16][17]}

La Telefonía IP es sólo un subconjunto de comunicaciones unificadas. Además de la integración de los servicios de voz con la red IP, también se pueden añadir servicios de presencia, mensajería instantánea, video y movilidad. Estos servicios, opcionales en este proyecto, se describen a continuación.

- **Presencia.** La mayoría de servicios de red funcionan sin que el usuario tenga noción de si la contraparte que desean contactar está donde se piensa, y menos aún, si estará en disposición de comunicarse. La presencia es concebida como una de las funciones básicas para los nuevos sistemas de comunicaciones. Resuelve el problema de la locación y disponibilidad de los participantes con lo que obviamente se agilizan las comunicaciones. Los estados básicos de un contacto que se muestran explícitamente son: disponible, ocupado, ausente o desconectado. Este estado generalmente lo lleva un solo dispositivo, como un celular, un teléfono IP, una computador de escritorio o portátil, etc. La locación del usuario se define normalmente por el dispositivo que muestra la etiqueta de “disponible”. Para este proyecto, los servicios de presencia se plasmarán junto con la mensajería instantánea.
- **Mensajería Instantánea** La mensajería instantánea es un servicio de red que permite a los usuarios el intercambio de mensajes en tiempo real. Al

ser combinada con los servicios de presencia, es considerada una potente herramienta de colaboración y productividad. Como su nombre lo indica, la mensajería instantánea demanda baja latencia. A pesar de que puede manejar mensajes de texto, audio y video, generalmente se limita al intercambio de mensajes de texto. El cliente de mensajería puede ser implementado en teléfonos o computadores, pero normalmente se lo hace para el computador por las capacidades multimedia que éste presenta. Permite a más de dos usuarios participar en una sesión de mensajería instantánea, conocida como “cuarto de *chat*”.

- **Video y movilidad.** Con la nueva infraestructura, los parámetros de calidad de servicio y los mecanismos de control, la red corporativa puede soportar más servicios que los planteados. Así el video y la movilidad del usuario se ven favorecidos. El cableado estructurado categoría 6 garantiza un mayor ancho de banda que el necesario para las transmisiones típicas de video. Previa planificación, la red también soporta puntos de acceso inalámbrico para que los usuarios autorizados accedan de forma segura y controlada a los servicios de red desde dispositivos móviles como computadores portátiles o teléfonos inteligentes.

3.2.4 DIMENSIONAMIENTO DE EQUIPOS DE LA RED LAN

En esta parte del diseño se procede a dimensionar la capacidad de los principales equipos que formarán parte de las redes LAN de Quito y Guayaquil. Los requerimientos para los diferentes equipos se muestran en el anexo L.

3.2.4.1 Servidores

Los servicios que actualmente no cuentan con el *hardware* apropiado en Quito son: el antivirus McAfee, aplicaciones *Thin-Client* y el correo electrónico. Actualmente, el servidor de correo electrónico está implementado en el mismo equipo que cumple las funciones de *firewall*, lo cual implica un riesgo de

seguridad y punto único de falla. Por esta razón se dimensionará un servidor exclusivo para el servicio de correo electrónico, de manera que el *firewall* se dedique expresamente a las funciones de seguridad. Para Guayaquil se debe dimensionar un servidor de archivos.

3.2.4.1.1 Servidor de aplicaciones *Thin-Client* ^{[40][41]}

El dimensionamiento del servidor que albergará los servicios de aplicaciones *Thin-Client*, requiere un análisis de *software* y *hardware*.

El sistema operativo de red *Microsoft Windows Server 2008* es compatible con los servicios *Thin-Client*, soportados con el *software XP-Unlimited*. Los requerimientos mínimos recomendados para *Microsoft Windows Server 2008* son: procesador *Intel Pentium/Celeron* o *AMD K6/Athlon/Duron* de 2 GHz, 2 GB de RAM y 40 GB de disco duro.

Generalmente los requerimientos de *hardware* para un producto de *software* determinado los especifica el fabricante. Sin embargo, es mejor basarse en estadísticas de la utilización actual del sistema. Con el uso de la herramienta de *software Everest Ultimate Edition 5* se desplegó la información de los procesos actuales y su ocupación de memoria RAM (ver anexo H), información importante para el dimensionamiento de la memoria RAM de un servidor. Los requerimientos de memoria son dependientes del número de usuarios. Para tareas regulares se requieren 96 MB de memoria RAM por usuario, mientras que tareas con funciones multimedia requieren 128 MB. Actualmente se tienen 2 equipos *Thin-Client*, pero se pretende incrementar el número a 5 en los próximos 5 años, por lo que en total se tendría un uso aproximado de memoria de 512 MB.

Se recomienda como mínimo una capacidad de almacenamiento en disco duro de 30 GB para el servidor de aplicaciones y por usuario una capacidad de 5 a 10 GB. En este caso con 5 *Thin-Client* se necesitan 50 GB de almacenamiento para usuarios. En total se necesitan 80 GB de espacio en el disco duro para el servicio de aplicaciones *Thin-Client*.

3.2.4.1.2 Servidor de Antivirus McAfee ^{[42][43]}

Para el servidor de antivirus McAfee se recomienda como mínimo el uso de *Microsoft Windows Server 2000* o superior. En este dimensionamiento se plantea el uso de *Microsoft Windows Server 2008*, como actualización y por ser compatible con el servicio de antivirus. Los requerimientos de *hardware* son los mismos especificados para el servidor *Thin-Client*.

Actualmente todos los procesos en memoria del servicio de antivirus McAfee tienen una ocupación en memoria de 190.4 MB.

3.2.4.1.3 Servidor de Correo ^[44]

El servidor de correo electrónico será dimensionado sobre el sistema operativo Linux Centos 5.6 por ser la versión estable más actual y por su facilidad para la migración del actual servicio de correo electrónico de *Sendmail* a *Qmail*. Los requerimientos recomendados para esta versión son: Intel x86-compatible (32 bit) (*Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP*) o AMD64 (*Athlon 64, etc.*) e *Intel EM64T*; 64 MB de RAM, 2 GB de disco duro.

Para el correo electrónico se necesita una capacidad de almacenamiento proporcional al número de cuentas de correo. Se establece que para administrar una cuenta de correo se necesitan 100 MB. Si actualmente se tienen 200 cuentas a nivel nacional y se prevé un crecimiento a 250 cuentas para los próximos últimos 5 años, se esperaría un total aproximado de 25 GB de espacio en el disco duro. En total entre todos los servicios se necesita un espacio mínimo de 20 GB por lo que se recomienda un disco duro con mayor capacidad de la esperada.

3.2.4.1.4 Servidor de Archivos ^{[45][46]}

El nuevo servidor de archivos será instalado en Guayaquil para servir a cerca de 36 usuarios en los próximos 5 años. Para este servidor, donde lo más importante

es la capacidad de almacenamiento, se puede utilizar un computador de escritorio de buenas características de *hardware* con un sistema operativo *Windows Server 2008*. La capacidad máxima de almacenamiento por usuario será de 2 GB, por lo que el servidor necesitará 72 GB sólo para almacenamiento de datos del usuario. Como el sistema operativo y otras funciones también ocupan espacio en disco, se requiere un disco duro de 120 GB como mínimo.

3.2.4.1.5 Servidor IPT

La central IP-PBX o servidor de Telefonía IP debe cumplir requerimientos técnicos mínimos para que su funcionamiento sea óptimo. En esta sección se analizan los requerimientos del servidor de Telefonía IP en base a funciones, estándares y protocolos actuales necesarios.

Para la integración del servidor de Telefonía IP a la red de datos, debe disponer de 2 puertos RJ-45 10/100/1000 Mbps, *auto-sense* y MDI/MDI-X. Si bien se mantendrá funcionando un puerto, el sobrante servirá como respaldo para cualquier eventualidad.

El número de llamadas simultáneas que debe soportar el servidor de Telefonía se considera para el peor de los casos, es decir, cuando todas las extensiones realicen una llamada. Por lo tanto se tendrán 52 llamadas simultáneas para Quito y 31 llamadas simultáneas para Guayaquil. Como el servidor de Telefonía IP es centralizado, el total de llamadas simultáneas a soportar será de 83.

La Telefonía IP permite implementar servicios más complejos que los servicios de voz tradicionales, pero que brindan mayor comodidad al usuario, entre las que se encuentran: la conferencia (mínimo para 3 usuarios), la capacidad de personalizar los *ringtones* y la música en espera (*music on Hold*), la característica de *find-me/follow-me* para no perder llamadas importantes, y finalmente la capacidad de almacenamiento de las llamadas no contestadas. Para el almacenamiento de las llamadas no contestadas es necesario que el número de buzones de voz sea igual o mayor que el número de extensiones.

También resulta necesario considerar la simultaneidad de acceso a las bandejas de correo. Se estima que alrededor de la quinta parte de los usuarios del servicio accederán al mismo tiempo. Por lo tanto, para Quito se estiman 11 usuarios simultáneos para la bandeja de correo, mientras que para Guayaquil se estiman 6 usuarios simultáneos.

3.2.4.2 Gateways de Voz ^{[47][48]}

Los dispositivos conocidos como *gateways* de voz y ATAs (figura 3.11) permiten la conversión entre códecs, protocolos y formatos de voz para interconectar diferentes sistemas de Telefonía. En este caso se necesitan *gateways* para los servicios de la PSTN para interconectar terminales telefónicos como máquinas de fax, teléfonos analógicos o teléfonos inalámbricos DECT. Estos dispositivos también cuentan con puertos RJ-45 para interactuar con la red de datos o troncales SIP.



Figura 3.11 Gateway HP VCX v7111 FXO/FXS y Cisco ATA 187

Los *gateways* tienen puertos FXS y FXO para dispositivos analógicos. Se requerirán 5 puertos FXS en Quito, para 4 faxes y 1 teléfono analógico; y 5 puertos FXS en Guayaquil, para 4 faxes y 1 teléfono inalámbrico DECT. El número de puertos FXO dependerá del número de líneas troncales analógicas que se requieran, de igual manera que con el número de puertos para troncales digitales E1.

3.2.4.3 Switches

Se requiere dimensionar la cantidad de *switches* para la capa de acceso, la cantidad de puertos por *switch* y sus velocidades de *backplane* y *throughput*.

3.2.4.3.1 Dimensionamiento de switches de capa acceso

El número de *switches* de acceso es proporcional a la cantidad de usuarios a los que se brindará el servicio. En Quito los *switches* de acceso se ubicarán en el cuarto de equipos, en el primer piso, y en el cuarto de telecomunicaciones, en la planta baja. El cuarto de equipos dará servicio a planta baja, primer piso y segundo piso, mientras que el cuarto de telecomunicaciones del subsuelo brindará servicio únicamente a esa área. En la tabla 3.12 se muestra el resumen del número de *switches* necesarios con su respectiva cantidad de puertos.

La tabla 3.12 indica que se necesitan 3 *switches* de 48 puertos, un *switch* de 24 puertos y un *switch* de 12 puertos para Quito. Para Guayaquil se necesita un *switch* de 48 puertos y uno de 24 puertos. Además, cada *switch* deberá disponer de 2 puertos adicionales que manejen velocidades de 10/100/1000 Mbps, conocidos como puertos de *uplink* para la interconexión entre la capa acceso y distribución.

Sucursal	Piso	Puntos Datos	Puntos Voz	# switches	# Puertos/switch
QUITO	SB	29	25	1	48
				1	12
	PB	20	22	1	48
	P1	24	23	1	48
	P2				
PI	9	9	1	24	
GUAYAQUIL	Ala 1	12	12	1	24
	Ala 2	18	19	1	48

Tabla 3.12 Cantidad de switches de acceso y números de puertos correspondientes

3.2.4.3.2 Dimensionamiento de switches de capa distribución

La LAN de Quito implementará la capa de distribución con 2 *switches* para redundancia. El número de puertos para estos *switches* depende del número de conexiones que tendrá con la capa acceso y con la capa núcleo. En la tabla 3.13

se muestra en resumen el número de puertos y las conexiones con los equipos de acceso para un solo *switch* de distribución, ya que el segundo *switch* es redundante. Según la tabla 3.13 se necesitan 2 *switches* con 8 puertos. No obstante, por motivos de crecimiento se dimensionará *switches* con 12 puertos con velocidad de transmisión de 10/100/1000 Mbps.

Etiqueta	Equipo conectado	Puertos necesarios	Puertos
SWUD1	SWUA1	1	Gi0/1
	SWUA2	1	Gi0/2
	SWUA3	1	Gi0/3
	SWUA4	1	Gi0/4
	SWUA5	1	Gi0/5
	SWUD1/2	1	Gi0/6
	SWUC	2	Gi0/7-Gi0/8
TOTAL		8	

Tabla 3.13 *Conexión y números de puertos para el switch de distribución*

3.2.4.3.3 *Dimensionamiento de switches capa de núcleo*

En el esquema planteado se requieren dos *switches* de núcleo, uno para Quito y otro para Guayaquil. Para Quito se dimensionó un *switch* de 14 puertos, y para Guayaquil un *switch* de 8 puertos. Por crecimiento se dimensionará un *switch* de 16 puertos para Quito y uno de 12 puertos para Guayaquil. En la tabla 3.14 se resume el número de puertos y conexiones necesarias para los *switches* de núcleo de Quito y Guayaquil.

Los *switches* de núcleo deberán resistir la mayor carga de tráfico ya que a estos irán conectados los servidores. Los servidores no se conectarán en la capa de distribución ya que algunos de los servicios son accedidos desde otras sucursales, lo cual puede provocar congestión innecesaria en el *backbone* de la red LAN Quito.

Etiqueta	Equipo conectado	Puertos necesarios	Puertos
SWUC	SWUD1	2	Gi0/1-Gi0/2
	SWUD2	2	Gi0/3-Gi0/4
	FW	1	Gi0/5
	AS-400	2	Gi0/6-Gi0/7
	SVR MAIL	1	Gi0/8
	SVR IPT1	1	Gi0/9
	SVR McAfee	1	Gi0/10
	SVR TNC	1	Gi0/11
	GWU1	1	Gi0/12
	SVRUIO	1	Gi0/13
	Router	1	Gi0/14
SWGC	SWGA1	2	Gi0/1-Gi0/2
	SWGA2	2	Gi0/3-Gi0/4
	SRVGYE	1	Gi0/5
	SRVVIDEO	1	Gi0/6
	GWG2	1	Gi0/7
	Router	1	Gi0/8

Tabla 3.14 Cantidad de puertos para los switches de núcleo

3.2.4.3.4 Dimensionamiento de la velocidad de backplane y throughput

Uno de los principales problemas en las redes es la congestión, debido principalmente a que los equipos no soportan la carga bajo la cual están trabajando. Para evitar este problema, en el diseño se debe dimensionar la velocidad de *backplane* y *throughput* de los *switches*.

En la tabla 3.15 se muestra en resumen la velocidad de *backplane* y el *throughput* o velocidad de envío de paquetes para los *switches* de la capa acceso, distribución y núcleo. En el anexo I se muestra un ejemplo de cálculo.

Es importante mencionar que las velocidades de *backplane* y *throughput* mostradas en la tabla 3.15 se dimensionaron para el peor de los casos, y sirven como parámetros de rendimiento para los *switches*.

Switch	#puertos 10 /100 [Mbps]	#puertos 10 /100/1000 [Mbps]	Velocidad backplane [Gbps]	Throughput [Mpps]
Acceso	12	2	6.4	4.8
	24	2	8.8	6.5
	48	2	13.6	10.1
Distribución	0	12	24	17.9
Núcleo	0	16	32	23.8

Tabla 3.15 *Resumen de las velocidades de backplane y throughput requerido*

3.2.4.4 Terminales Telefónicos IP

Los terminales telefónicos IP a utilizarse deberán ser compatibles con el sistema telefónico y soportar las funciones de Telefonía requeridas en este diseño. El tipo de teléfono IP dependerá del tipo de usuario.

Los teléfonos IP se han clasificado en: terminales gerenciales, terminales gama media y recepción. Los terminales gerenciales como su nombre lo indica, serán distribuidos para la utilización de los gerentes de la matriz Quito y sucursal Guayaquil. Los terminales de gama media serán utilizados por el personal de operaciones y mantenimiento de Seguros Alianza. Finalmente, los terminales de recepción, se dispondrán para los usuarios que trabajan en la sala de recepción de las agencias. Se necesitará de una botonera para manejar las llamadas entrantes y salientes hacia las distintas extensiones.

Los terminales telefónicos IP tendrán 2 conectores mini jack-RJ45 con *switch* interno, para el servicio de voz y datos. Además, es necesario considerar el soporte de la tecnología PoE y la capacidad de brindar calidad de servicio. En la tabla 3.16 se muestra el número de terminales telefónicos según su clasificación.

Se reutilizarán las máquinas de fax, un teléfono analógico y un teléfono inalámbrico DECT, conectados con ATAs. Para el caso especial de la extensión del presidente de Alianza, que reside en España se manejará un *softphone*, capaz

de ser instalado en cualquier computador, de preferencia compatible con el sistema operativo *Microsoft Windows XP* o superior.

Sucursal	Gama Alta	Gama Media	Softphone	Recepción	Botonera:	ATA
Quito (Matriz)	7	42	1	1	Una para 50 extensiones	5
Guayaquil (centro)	4	25	0	1	Una para 30 extensiones	5
TOTAL	11	67	1	2	2	10

Tabla 3.16 *Número de terminales telefónicos IP*

3.2.5 DIAGRAMA DE RED

La figura 3.12 contiene la topología propuesta para la red corporativa. En esta figura se pueden apreciar todos los componentes que conforman la red corporativa, pasando por la LAN de Quito, LAN de Guayaquil, enlace WAN entre las dos sucursales, y la ubicación de otros elementos, como el *firewall* y los *gateways* de voz para la conexión con la PSTN.

3.3 DIMENSIONAMIENTO DEL ENLACE WAN QUITO-GUAYAQUIL Y ACCESO A LA PSTN

Como parte de la reingeniería de la red de Alianza, es necesario redimensionar la capacidad de los enlaces WAN y el enlace de Internet para la transmisión de los nuevos servicios a implantarse. Para el diseño es necesario considerar la ubicación de las sucursales que se van a interconectar, el dimensionamiento de la capacidad del enlace WAN en base a los servicios a transportar, la tecnología que se utilizará como última milla en la interconexión y finalmente el costo.

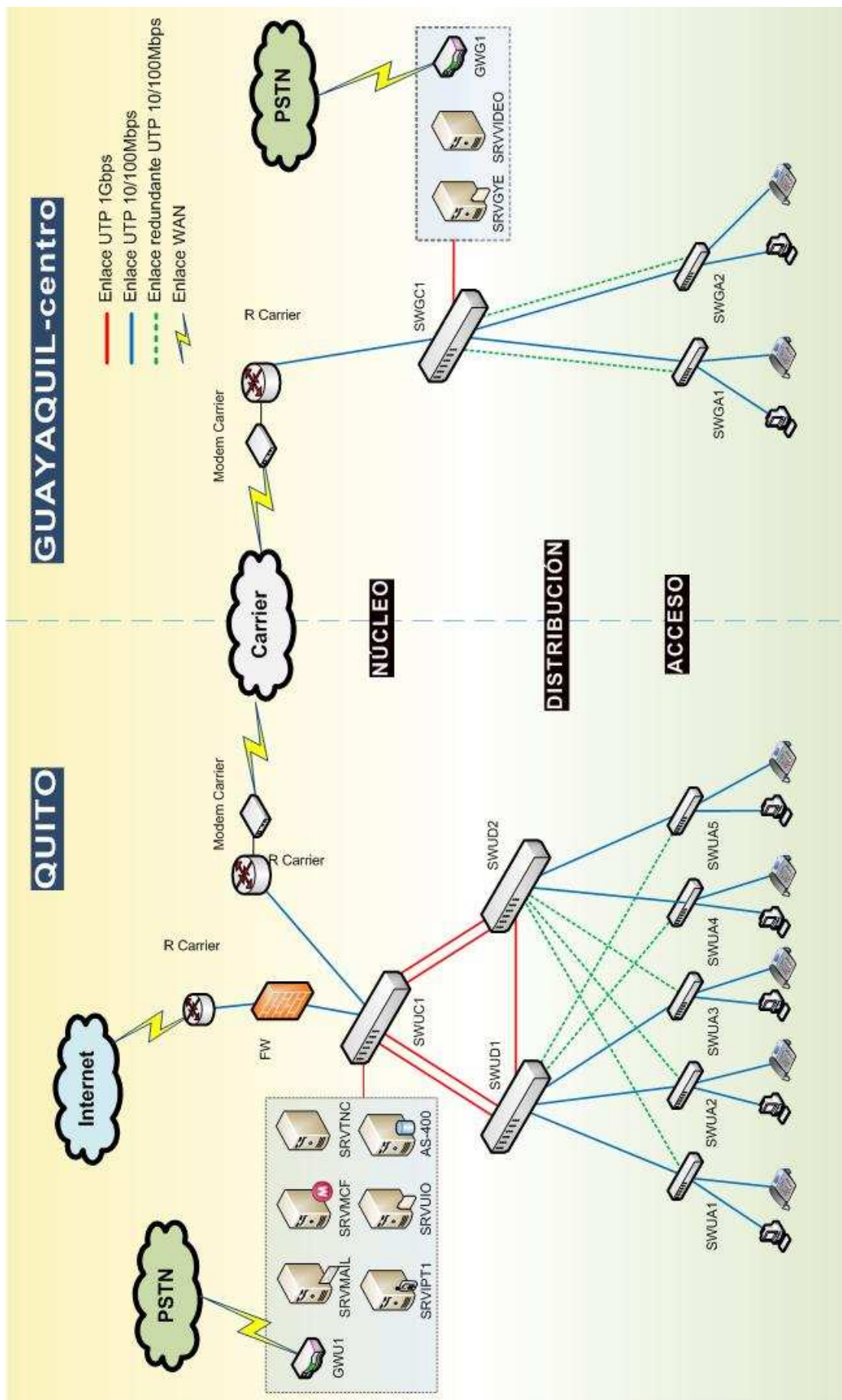


Figura 3.12 Topología propuesta para la Red Corporativa de Alianza de Seguros

3.3.1 UBICACIÓN DE LAS SUCURSALES

Como se mencionó en el capítulo anterior, Alianza tiene sucursales a nivel nacional. Sus oficinas están ubicadas en ciudades como: Quito, Guayaquil, Cuenca, Manta, Santo Domingo, Machala y Milagro. La matriz ubicada en Quito concentrará la mayor parte de los servicios de red y sobre todo el acceso a Internet, siendo necesaria la conexión de todas las sucursales hacia la matriz con una topología en estrella. Para el dimensionamiento WAN se necesitará conocer el número de usuarios que corresponde a cada sucursal (ver tabla 3.17).

Sucursal	Número Empleados	Crecimiento
Quito (Matriz)	56	64
Guayaquil Centro	30	35
Cuenca	20	23
Manta	11	13
Santo Domingo	8	9
Milagro	6	7
Guayaquil Kennedy	6	7
Machala	4	5

Tabla 3.17 *Ubicación y crecimiento de las sucursales de Alianza*

3.3.2 DIMENSIONAMIENTO DE ENLACES

El dimensionamiento de la capacidad del enlace WAN depende principalmente del tipo de aplicaciones que se utilizarán para cada servicio. El tipo de aplicaciones consecuentemente definirá el tipo de tráfico y sus características, como la tolerancia a errores, la sensibilidad al retardo y el ancho de banda.

3.3.2.1 Tolerancia a Errores

Las aplicaciones tolerantes a errores son aquellas que soportan cierto grado de retransmisión, cuando por cualquier motivo se presentan errores en las tramas o se las descarta. Las aplicaciones no tolerantes a errores, al contrario, son aquellas que no funcionarán bien si se requieren constantes retransmisiones.

3.3.2.2 Sensibilidad al Retardo

Existen aplicaciones sensibles al retardo como son las aplicaciones en tiempo real, las cuales requieren un retardo mínimo y constante; mientras que otras aplicaciones, como la navegación WEB, no son sensibles al retardo o a su variación.

3.3.2.3 Ancho de Banda

El ancho de banda es una importante característica para el correcto funcionamiento de las aplicaciones. El ancho de banda puede ser elástico o no elástico. Las aplicaciones elásticas como las aplicaciones WEB operan con cualquier ancho de banda que se les ofrezca; mientras que las aplicaciones no elásticas como la Telefonía IP, requieren un ancho de banda mínimo garantizado.

En la tabla 3.18 se muestra en resumen el tipo de tráfico a cursar por la red WAN y sus características, evaluadas según las consideraciones antes mencionadas.

Aplicación\Tipo de tráfico	Ancho de banda	Tolerancia a errores	Sensibilidad al Retardo
Actualización de Antivirus	Elástico	No tolerante	No sensible
Correo electrónico	Elástico	No tolerante	No sensible
Web	Elástico	Tolerante	No sensible
Telefonía IP	No elástico	Tolerante	Sensible
Transacciones BDD	Elástico	No tolerante	No sensible
Escritorio Remoto	Elástico	No tolerante	No sensible
Video	No elástico	Tolerante	Sensible

Tabla 3.18 *Tipo de tráfico a cursar por la red WAN y sus características*

De la tabla 3.18 se concluye que el tráfico que necesita mayores medidas de calidad de servicio es el de Telefonía IP y Video.

El nivel de importancia y utilización de las aplicaciones también son factores importantes para el diseño de los enlaces. La Telefonía IP es la aplicación con mayor importancia por ser sensible al retardo y por la necesidad de tener un ancho de banda fijo. Mientras tanto, de las aplicaciones analizadas en el capítulo 2, se observa que las transacciones de base de datos son las más importantes para la empresa y éstas se realizan en horario laboral de 8h30 a 17h30 provocando un tráfico densamente pequeño; las aplicaciones de correo electrónico, acceso a Internet y escritorio remoto se consideran de mediana importancia y utilización, y finalmente la actualización de antivirus es una aplicación de baja utilización y con gran cantidad de tráfico.

El tráfico generado por el video a tiempo real del servidor ubicado en Guayaquil se considera de baja utilización porque el acceso al sistema se lo realizará esporádicamente, además por políticas de la empresa el Gerente General es el único que podría acceder al servicio desde las oficinas en Quito. Se considera también que las actualizaciones de antivirus se deben configurar para que su funcionamiento sea en horas de menor congestión de la red WAN, de esta manera no influirá en el ancho de banda total de los enlaces WAN.

En base a lo considerado anteriormente se procede a estimar el tráfico para el dimensionamiento de los enlaces. Se utilizarán los cálculos de estimación de tráfico ya realizados para la velocidad de cada servicio mostrado en la tabla 3.18. Adicionalmente de lo analizado en la sección 2.3.2.2 del capítulo 2 respecto a las consideraciones de Telefonía IP donde se comprobó que el códec G.729 presenta buenas características de retardo y menor consumo de capacidad del canal, éste será el códec a utilizar para la transmisión de voz.

Para determinar el número de usuarios simultáneos se tomaron las siguientes consideraciones:

- Al servicio de video únicamente tiene acceso el Gerente General de la empresa, si éste se encuentra en la ciudad de Quito podrá acceder al servicio remoto ubicado en Guayaquil.
- Al servicio de correo electrónico acceden simultáneamente 3 usuarios.
- En el caso de acceso hacia Internet se ha considerado compartir el ancho de banda en una relación de 8 a 1; de esta manera se dividió el número total de usuarios para 8 obteniendo el número de usuarios simultáneos.
- El número de canales simultáneos de voz para Telefonía IP es de 4, según el análisis previo realizado en la sección 2.3.3 y que se resume en la tabla 2.32: tráfico proyectado y circuitos recomendados.
- Las transacciones de base de datos son las más importantes y es donde más utilización se tiene, por lo que se determinó que en la hora pico aproximadamente la mitad del total de usuarios es simultánea.
- Las actualizaciones del servicio de antivirus se programarán para que se realicen en un horario fuera de oficina, por lo que no se considerará dentro de la simultaneidad del enlace WAN.
- Finalmente, el escritorio remoto es una aplicación que facilita al personal del Área de Sistemas brindar soporte remotamente, por lo que se considera que máximo existirá un usuario conectado a un equipo.

Según las consideraciones anteriores, en la tabla 3.19 se presenta el ancho de banda requerido por tipo de tráfico para el enlace Quito-Guayaquil.

Tipo de tráfico	Ancho de banda por aplicación	# de usuarios simultáneos	Ancho de banda requerido [kbps]
Vídeo	115	1	115
Correo electrónico	1,45	3	4,35
Web	182,1	5	910,5
Telefonía IP	25,6	4	102,4
Transacciones BDD	9,953	18	179,154
Escritorio remoto	83,92	1	83,92
		TOTAL	1395,33

Tabla 3.19 *Ancho de banda requerido según el servicio de red para el enlace Quito-Guayaquil*

El tráfico de Telefonía IP y video sólo se tomará en cuenta para el dimensionamiento del enlace WAN Quito-Guayaquil, ya que el resto de sucursales se encuentra fuera del alcance de este proyecto. El anexo J muestra el ancho de banda requerido para los enlaces de las demás sucursales según el tipo de servicio.

3.3.3 TECNOLOGÍA WAN A UTILIZARSE

Los *carriers* e ISPs cuentan hoy en día con diferentes tecnologías WAN en su nube de servicio. También manejan variedad de medios de transmisión para el acceso de sus clientes, conocido como última milla. Es importante considerar que dependiendo de la tecnología y el medio de transmisión variará su costo. A continuación se analizan las diferentes tecnologías y medios de transmisión disponibles para adecuar a las necesidades de Seguros Alianza.

Entre los medios de transmisión disponibles para el diseño se encuentran:

- **Cobre.** Es el medio de transmisión más común que ofrecen los *carriers* para sus enlaces de última milla por su bajo costo y fácil instalación. Presenta problemas de interferencia, ruido, latencia y *jitter* provocando errores en las comunicaciones.
- **Fibra Óptica.** Medio de transmisión que no presenta problemas de interferencia electromagnética. Es un medio de transmisión más confiable y eficiente que permite alcanzar grandes capacidades de transmisión, pero su costo es alto y es de difícil instalación. Se necesitan equipos que soporten la comunicación con este medio de transmisión y de *transceivers* que hagan la respectiva conversión eléctrico/óptica.
- **Radio enlace.** Medio de transmisión no guiado que posibilita las comunicaciones en lugares donde no se puede acceder fácilmente con medios de transmisión guiados. Trabaja a frecuencias de 5.4 Ghz y 5.8 GHz. Sus principales desventajas son las pérdidas y posibles errores de transmisión debidos a la interferencia.

El medio de transmisión preferencial para este proyecto será la fibra óptica, por las ventajas que presenta. En caso de no poder acceder a este medio de transmisión en alguna sucursal, se utilizará el cobre.

La tecnología WAN que se utilice depende del proveedor de servicios, actualmente se utilizan como última milla enlaces dedicados con *Frame-Relay* y *ADSL (Asymmetric Digital Subscriber Line)*.

Con estas consideraciones de tecnología y medio de transmisión para el enlace WAN se prevé que se necesitará un *router* en cada sucursal con sus respectivos *transceivers*. La fibra óptica del proveedor llegará hasta el *transceiver* y mediante cable UTP con conectores RJ-45 se realizará la conexión al *router* proporcionado por el proveedor de servicios. A su vez el *router* se conectará por otra interfaz de red a la red LAN por medio de cable UTP con conectores RJ-45. En la figura 3.13 se muestra el esquema de los enlaces WAN.

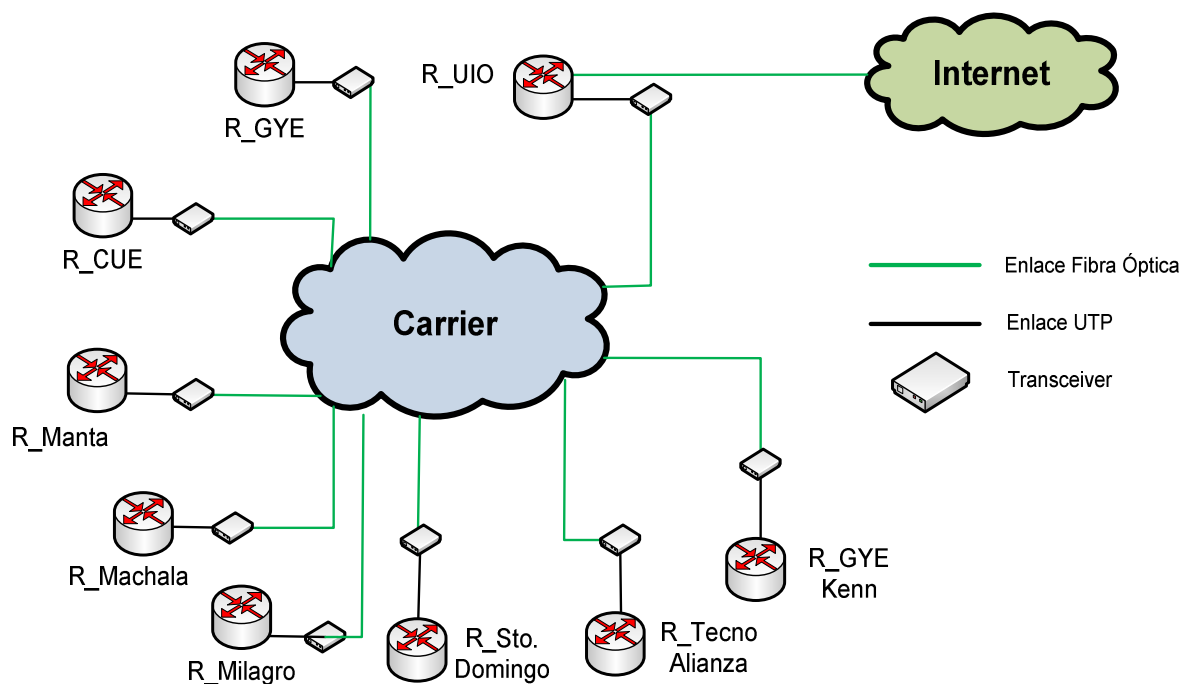


Figura 3.13 Esquema de enlaces WAN

3.3.4 CAPACIDAD DEL ENLACE WAN

Debido a la topología en estrella, el enlace de Quito hacia el *carrier* deberá ser la suma de todos los enlaces. En la tabla 3.20 se muestra un resumen de las capacidades necesarias para todos los enlaces hacia el *carrier*.

AGENCIA	ANCHO DE BANDA
GYE PRINCIPAL	1,5 Mbps
GYE KENNEDY	512 kbps
MACHALA	256 kbps
QUITO MATRIZ	5 Mbps
MILAGRO	512 kbps
CUENCA	1024 kbps
MANTA	512 kbps
SANTO DOMINGO	512 kbps

Tabla 3.20 *Resumen de las capacidades necesarias para todos los enlaces hacia el carrier*

Finalmente, en este análisis de tráfico WAN hace falta realizar el cálculo del enlace hacia Internet que podría ser proporcionado por el mismo *carrier* o a su vez por una empresa dedicada a brindar el servicio de Internet o ISP. Para el cálculo del enlace hacia Internet es necesario tomar en cuenta el tráfico de correo electrónico del tipo WEB que generará la matriz Quito. Estos valores son resumidos en la tabla 3.21.

Tipo de tráfico	Ancho de banda por aplicación [kbps]	# de usuarios simultáneos	Ancho de banda requerido [kbps]
Correo electrónico	1.45	5	7.25
Web	182.1	8	1465.91

Tabla 3.21 *Resumen del tráfico generado por la matriz de Quito hacia Internet*

La capacidad necesaria para el enlace de Internet se determina mediante la suma de todo el tráfico que se genere hacia Internet. Por tal razón, en el cálculo intervendrán el tráfico de correo electrónico y el tráfico WEB de todas las oficinas. El total resultante es de 3845.13 kbps de capacidad (tomando en cuenta los valores de la tabla 3.19 y las tablas del anexo J), por lo que se solicitará un canal hacia Internet de 4096 kbps, valor estandarizado disponible en el mercado.

3.3.5 CONDICIONES DE SERVICIO PARA EL SLA

El proveedor de servicios deberá cumplir con los requerimientos mínimos necesarios considerados para que Seguros Alianza obtenga disponibilidad de sus servicios, confiabilidad, buenos tiempos de respuesta y niveles de servicio y operación acorde a la criticidad de los servicios que se transmiten por los enlaces WAN.

Para los enlaces con los sucursales se necesita una compartición de datos de 1:1 y para el servicio de Internet se requiere también una compartición de 1:1.

Por parte del operador de servicios se deberá ofrecer mínimo una disponibilidad de 99.6% al año para los servicios de Internet y última milla. El retardo en el enlace nacional no será mayor a 30 ms y con una pérdida de paquetes cercana al 0%, para la correcta transmisión de voz.

El tiempo de respuesta para una falla del servicio no deberá superar los 120 minutos máximo más el tiempo de desplazamiento de los técnicos a las oficinas del cliente. El tiempo de respuesta para caídas de última milla será de 2 horas a nivel nacional. En caso de un daño en el equipo y se necesite el reemplazo del mismo, el tiempo en que se deberá demorar el cambio de equipo contando desde la caída del servicio hasta el levantamiento del mismo, no sobrepasará las 2 horas.

El soporte técnico que se necesita actualmente es de 24 horas del día, los 7 días de la semana, los 365 días del año, por la criticidad del servicio de base de datos, que concentra toda la información de los seguros.

El cliente, en este caso Alianza de Seguros, brindará toda la apertura del caso para realizar las instalaciones de los equipos. La infraestructura civil, acometidas internas u otras obras civiles dentro de la edificación serán responsabilidad de la empresa. Además, brindará las facilidades para la conexión a una toma eléctrica con conexión a tierra, regulada y/o respaldada por UPS para la conexión de los equipos del proveedor.

3.3.6 ACCESO A LA PSTN

Para el acceso a la PSTN se plantea el uso de troncales SIP, por sus ventajas en escalabilidad, flexibilidad y costos, ofrecidas por la CNT. Estas troncales SIP ingresarán directamente a los servidores de Telefonía IP a través de puertos RJ-45 que soporten troncales SIP. Para la ciudad de Quito se necesitan 15 troncales SIP y para Guayaquil, 19 troncales SIP.

La empresa CNT se encargará de realizar las configuraciones necesarias para la conexión. En los *gateways* se requiere el soporte nativo de troncales SIP RFC2833. Se necesitarán 8 puertos FXO en cada localidad. Cuatro de éstos se utilizarán para conectar las líneas de fax, y 4 como respaldo de las troncales SIP. También se requerirá el soporte modular para puertos E1, BRI, PRI, FXO, FXS para futuros cambios o adiciones.

3.4 DISPONIBILIDAD

Alianza de Seguros depende de sus recursos tecnológicos para realizar sus operaciones día a día. Algunos servicios de red son cruciales y deben estar en funcionamiento con la mayor disponibilidad posible; en particular, el servicio telefónico y el de base de datos que son los más importantes. Según datos de la

empresa, estos dos servicios pueden estar fuera de funcionamiento como máximo media hora al día sin que se presenten pérdidas considerables. Esto significa que la pérdida de estos dos servicios no deben superar las 15 horas en una base de 30 días, lo que equivale a una disponibilidad de al menos el 97.9%.

El método más común para aumentar la disponibilidad es la redundancia. Sin embargo, no se puede replicar cada elemento de la red por el elevado costo que esto implica, sino que se deben aislar los principales puntos de falla.

El normal funcionamiento de los servicios de la red corporativa se puede ver afectado de forma considerable si falla cualquiera de los siguientes elementos:

- Conectividad a nivel LAN
- Enlace WAN
- Acceso a la PSTN
- Suministro de energía eléctrica

3.4.1 REDUNDANCIA EN LA RED CORPORATIVA

En la sección de diseño se describió el uso de *switches* y enlaces redundantes en las diferentes capas de las LAN de Quito y Guayaquil, enfocados a aumentar la disponibilidad de la red a nivel local. A esto se debe agregar el uso de fuentes de poder redundantes para los *switches* de núcleo. Con estas medidas se garantiza que los usuarios puedan realizar sus labores de forma casi ininterrumpida. Los usuarios remotos de Guayaquil usan el enlace WAN para acceder a los servicios centralizados de Quito.

La disponibilidad que ofrecen la mayoría de ISPs en el país es del 98.6% mensual, lo cual supera el 97.9% requerido. Por esta razón no se propondrá la redundancia del enlace WAN.

El sistema telefónico se ve directamente afectado si existen fallas en: el servidor de Telefonía IP, los *media gateways*, el enlace WAN o el acceso a la PSTN. En el

servidor de Telefonía IP y los *media gateways* se pueden usar fuentes de poder y/o discos duros redundantes, además de los respaldos de la información. Con esto se mitiga la falla del servicio telefónico debido a estos elementos. De presentarse una falla en el enlace WAN, el servidor de Telefonía IP perdería contacto directo con Guayaquil. En este caso, el *media gateway* de esta localidad puede tomar el control de las llamadas y enrutarlas a la PSTN, con lo que se restaura la comunicación entre la matriz y la sucursal. El acceso a la PSTN es independiente en cada localidad. Si uno de los dos accesos falla, las llamadas se pueden enrutar a través del enlace WAN y salir por el acceso a la PSTN disponible de la otra localidad.

Para el servicio de Telefonía IP se consideran dos servidores, uno en la matriz y otro en la sucursal de Guayaquil, con lo que se consigue tolerancia a fallos del enlace WAN, de la PSTN y del servidor de Telefonía IP. La primera ventaja de este esquema es la redundancia geográfica. El servidor de la sucursal es respaldo del servidor de la matriz y viceversa. En caso de falla o mantenimiento de uno de los dos servidores, el otro puede tomar el control de las llamadas de las dos localidades, de preferencia en un lapso menor al de media hora. La segunda ventaja es que se descongestiona el enlace WAN. Con el servidor de Telefonía IP de la sucursal, todo lo relacionado con las llamadas se controla y se almacena a nivel local. Gracias a esto, el enlace WAN requiere menor capacidad y por lo tanto, se reduce su tarifa mensual.

Es importante mencionar que la información sensible contenida en los servidores de Telefonía, como la configuración de las cuentas de usuario, el registro de llamadas, las estadísticas del servicio, entre otros, se puede respaldar entre los dos servidores de forma opcional, en horarios que no afecten la jornada laboral. Los otros servidores de la red cuentan con partes redundantes, como fuentes de poder o discos duros, y con respaldos de su información a través de unidades de almacenamiento externas.

3.4.2 SUMINISTRO DE ENERGÍA ELÉCTRICA Y AIRE ACONDICIONADO

El suministro de energía eléctrica es uno de los puntos fundamentales para mantener a una red completamente operativa. La discontinuidad de este servicio y las variaciones en la electricidad pueden ocasionar daños en los equipos. Para mantener la operatividad de la red y evitar daños en los equipos por fallas de energía, se considerarán: el uso de PoE para los teléfonos IP, un suministro de potencia ininterrumpido UPS (*Uninterruptible Power Supply*) y una planta eléctrica a diesel, ya existente en la empresa.

3.4.2.1 PoE (*Power over Ethernet*)^{[49][50][51]}

Con la finalidad de garantizar un servicio telefónico ininterrumpido y una administración más efectiva disminuyendo la cantidad de cables, los teléfonos IP se alimentarán de energía eléctrica mediante PoE. Este estándar define dos elementos: el equipo de suministro de energía PSE (*Power Source Equipment*) y el equipo energizado PD (*Powered Device*). Los *switches* de acceso actúan como PSE y los teléfonos IP como PD. El estándar 802.3af clasifica a los equipos energizados según la potencia consumida, como se indica en la tabla 3.22.

Clase	Uso	Mínimo Nivel de Potencia a la salida del PSE [w] ⁸	Máximo Nivel de Potencia en el PD [w]
0	Por defecto	15.4	0.44 a 12.95
1	Opcional	4.0	0.44 a 3.84
2	Opcional	7.0	3.84 a 6.49
3	Opcional	15.4	6.49 a 12.95
4	Reservado para uso futuro	Se trata como Clase 0	Reservado para uso futuro

Tabla 3.22 Clasificación de PSE y PD en el estándar IEEE 802.3af

En general, la mayoría de teléfonos IP corresponde a las clases 2 y 3, con un consumo de potencia de 4 y 7 vatios respectivamente.

⁸ [w]:vatio, unidad de medida de potencia eléctrica

Para aminorar costos, la mitad de los puertos del *switch* tendrán PoE, que es la configuración por defecto en la mayoría de fabricantes de equipos de conectividad. Habrá la alternativa de que los teléfonos IP se conecten a la toma regular de voltaje con su respectiva fuente de poder, aumentando así la disponibilidad del servicio telefónico.

3.4.2.2 UPS (*Uninterruptible Power Supply*) ^[52]

El sistema UPS ayuda a proteger los equipos más importantes de la red durante fallas de energía eléctrica o a mantenerlos activos cuando existen cortes de energía, hasta que se ponga en funcionamiento la planta eléctrica de la empresa. Los equipos que más requieren el respaldo de energía son: servidores, *switches*, *routers* y *firewalls*. Adicionalmente, el uso de PoE implica que los teléfonos IP dependerán de la electricidad que les suplan los *switches* de acceso, por lo que esta potencia adicional debe ser tomada en cuenta para dimensionar el UPS.

En la tabla K.1 anexo K se resumen los equipos a proteger y sus requerimientos de potencia para Quito y Guayaquil. Se considera el uso de PoE solamente en la mitad de los puertos de acceso. Se considera un 20% de carga extra para crecimiento y para aumentar el tiempo que el UPS mantendrá activos a los equipos (10 minutos aproximados). Los resultados se expresan en kilovatios [kw] y kilovoltamperios [kVA] con un factor de potencia de 0.8 (valor aceptado para la eficiencia energética). Como resultado final del anexo K, se necesitan dos UPS de al menos 8.5 kVA y 4 kVA para Quito y Guayaquil respectivamente.

3.4.2.3 Planta de Energía Eléctrica a Diesel

Debido a los inesperados cortes en el servicio de energía eléctrica, se tiene una planta que suple al menos 3 horas de energía ininterrumpida al edificio y con ello, a los equipos de conectividad, hasta que se normaliza el servicio en la red. En Guayaquil no se contará con planta de energía eléctrica debido a que no se cuenta con el espacio físico para su implementación. Mientras ocurre el cambio

entre la energía de la red eléctrica pública y la planta privada, se cuenta con el respaldo del UPS.

3.4.2.4 Aire Acondicionado ^{[4][53][54]}

En el cuarto de equipos de Quito, donde se concentran la mayor cantidad de equipos de la red, estará instalado el sistema de aire acondicionado para mantener una temperatura entre 18 y 24°C y una humedad relativa del 30 al 50%. La unidad de disipación de calor es el BTU (*British Thermal Unit*) y se utiliza para dimensionar la capacidad del aire acondicionado en BTU por hora, la cual se obtiene con la siguiente expresión:

$$DT = PT_{eq} \times 3.413 + (1.25 \times A \times \Delta T)$$

donde: DT : Capacidad de disipación total del aire acondicionado en [BTU/h]
 PT_{eq} : Potencia total de los equipos en [w]
 A : Área total de las superficies del cuarto de equipos en [pie²]
 ΔT : Diferencia entre la temperatura externa al cuarto T_o y la temperatura interna deseada en el cuarto T_i en [°F]

En la tabla K.2 del anexo K se tienen las características físicas y térmicas del cuarto de equipos más el resultado de la capacidad necesaria de aire acondicionado. Como resultado, el aire acondicionado deberá tener una capacidad mínima de disipación de calor de 35000 BTU/h.

3.5 CALIDAD DE SERVICIO

La calidad de servicio tiene que ver con el trato diferencial que se da a cada servicio y cómo se les provee de los recursos necesarios para su correcto

funcionamiento. Para que la calidad de voz en la red corporativa sea similar o mejor que la de Telefonía tradicional, se toman en cuenta los siguientes aspectos: segmentación, priorización de tráfico, retardos y aprovisionamiento de recursos.

3.5.1 SEGMENTACIÓN Y PRIORIZACIÓN DE TRÁFICO ^{[18][22][55][56]}

Uno de los primeros pasos para diferenciar el tráfico de voz es segmentar la red LAN en varios dominios de colisión con VLANs. Además de evitar la propagación del *broadcast* del segmento de datos en el de voz, esta separación permite discriminar de qué dispositivo es el tráfico, si de un teléfono o un computador por la VLAN a la que éste pertenece, y así darle un trato diferenciado.

Dentro de la etiqueta de la VLAN se encuentran 3 bits que sirven para dar prioridad a cada trama 802.3 dentro de la red LAN. Estos bits son controlados por el protocolo IEEE 802.1p y representan la clase de servicio CoS, cuyos valores se muestran en la tabla 3.23 en orden de prioridad ascendente. Nótese que el valor 0 tiene un orden de prioridad mayor que el valor 2. Una prioridad más alta implica una transmisión más rápida de esa trama, una prioridad más baja en cambio, que la trama puede ser descartada en caso de congestión.

Los *switches* de la red LAN deberán manejar los valores mostrados en la tabla 3.23 o al menos soportar 2 colas de prioridad y así diferenciar voz y datos.

Bits	Prioridad de Usuario	Clase de Servicio (CoS)	Tipo de Tráfico
001	1 (Prioridad mínima. Trama descartable)	0	<i>Background</i>
010	2	1	Repuesto/Disponible
000	0 (Por defecto)	2	Mejor esfuerzo
011	3	3	Excelente esfuerzo
100	4	4	Carga controlada
101	5	5	Video interactivo, latencia y <i>jitter</i> menor a 100 ms
110	6	6	Voz interactiva, latencia y <i>jitter</i> menor a 10 ms
111	7 (Prioridad máxima)	7	Control de la red

Tabla 3.23 Valores de prioridad del protocolo 802.1p

Los mecanismos de calidad de servicio hasta aquí descritos, trabajan a nivel de capa 2, por lo que son útiles únicamente en la LAN. Para una clasificación y priorización de tráfico que pueda atravesar la red corporativa, existe el campo de servicios diferenciados DSCP (*Differentiated Services Code Point*) dentro de la cabecera del paquete IPv4. De este campo de 8 bits, se utilizan los 6 más significativos para la clasificación y los 2 restantes para control de flujo. La tabla 3.24 muestra las equivalencias entre los valores de precedencia CoS y los valores DSCP.

Capa 2 - CoS	Capa 3 - DSCP	Aplicación
0	0	Datos del mejor esfuerzo
1	10,14,16	Datos de prioridad media
2	18,20,22	Datos de alta prioridad
3	26	Señalización de llamadas (SIP, H.323)
4	34	Video Conferencia
5	46	Portadora de voz (RTP)
6	48-55	Reservado
7	56-63	Reservado

Tabla 3.24 *Equivalencia entre valores CoS y DSCP*

Se recomiendan los valores DSCP de 46 para el transporte de la voz, 26 para la señalización de Telefonía, 22 para servicios en general y 16 para gestión de red (SNMP).

Con el mapeo de CoS a DSCP ya se puede establecer la priorización de tráfico básica para toda la red corporativa de Alianza de Seguros. La etiquetación empezará desde los *switches* de acceso. Con cada puerto asignado a una VLAN de voz o datos se sabrá si el tráfico es generado por un computador o un teléfono. Con esta información, se define el valor del campo CoS. Una vez que las tramas lleguen al límite de la red y se deba pasar de la capa 2 a la 3, se traduce el valor CoS a su equivalente DSCP, se marca el paquete IP y viaja a través de la red del *carrier*. De vuelta en el límite de la LAN de destino, se hace el mapeo inverso de valores y las tramas llegan al dispositivo terminal. Este proceso se visualiza en la figura 3.14.

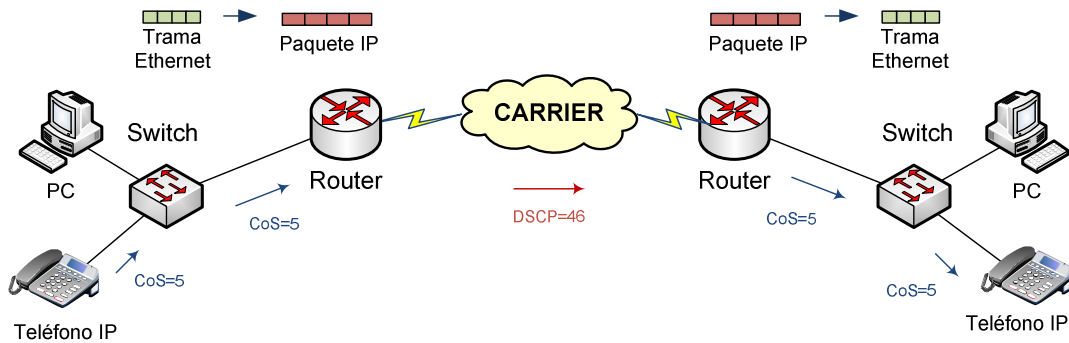


Figura 3.14 *Priorización de tráfico a través de la red corporativa*

Se prefiere que la red del *carrier* soporte MPLS ya que fue diseñado con criterios de diferenciación de servicios y otras prestaciones para calidad de servicio.

3.5.2 RETARDOS ^{[19][22]}

En el estándar G.114 de la ITU-T se recomienda que el retardo máximo para las transmisiones de voz, extremo a extremo y en un solo sentido, sea de 150 ms, de modo que la calidad auditiva sea aceptable. En la red corporativa el retardo se introduce principalmente por: codificación de voz, encolamiento, serialización y *buffer* de *jitter*. A continuación se describen estos factores y las técnicas para disminuir su efecto en el retardo.

3.5.2.1 Codificación de la Voz

Dependiendo del códec utilizado, el proceso de la codificación de la voz puede introducir mayor o menor retardo. Como ejemplo, el códec G.729 tiene un retraso de 25 ms al tomar dos muestras de voz de 10 ms cada una. El códec G.711 es más simple por lo que su retardo es menor.

3.5.2.2 Encolamiento

En caso de congestión, los paquetes generalmente forman colas en los *routers* del enlace WAN, por lo que se retrasa su envío. Es conveniente utilizar

combinaciones de los mecanismos de manejo de colas como PQ (*Priority Queueing*), CBQ (*Class Based Queueing*) o WFQ (*Weighted Fair Queueing*). Con ello se asegura que los paquetes de voz se envían primero incluso si existe congestión, con lo que el retardo por encolamiento es mínimo.

3.5.2.3 Serialización

A nivel de capa enlace, cada trama se transmite una tras otra consecutivamente. Si entre dos tramas de voz, de pequeña longitud, se transmite una trama de datos muy extensa, se corre el riesgo de que el retardo entre las tramas de voz supere los 150 ms. Para evitar esto sobre todo en el enlace WAN, se deben fragmentar las tramas de datos muy largas e intercalar las tramas de voz para que el retardo entre ellas sea tolerable.

3.5.2.4 Buffer de Jitter ^{[19][22]}

El *jitter* es la variación en el retardo. Cuando las tramas de voz llegan al dispositivo de destino, éstas se almacenan en un *buffer* que se va vaciando de tal manera que la señal de voz sea fluida y constante. Si las tramas llegan de forma irregular, es decir con *jitter*, es necesario almacenar mayor o menor número de tramas para dar la misma fluidez a la señal de audio entregada. La solución para este comportamiento es un *buffer de jitter* dinámico. El tamaño del *buffer* dinámico se ajusta según el comportamiento de la red, crece o se contrae en base a las marcas de tiempo de los paquetes RTP.

3.5.3 APROVISIONAMIENTO DE RECURSOS ^{[22][57]}

Más allá del manejo de prioridades y disminución del retardo, es crucial dotar a cada servicio del ancho de banda necesario, limitarlo y controlarlo, de manera que no se produzcan colas ni descarte de paquetes, en la medida de lo posible. Estas medidas son necesarias particularmente en el enlace WAN, donde es más probable que se produzcan los “cuellos de botella” de la red corporativa.

En la sección de dimensionamiento del enlace WAN se estableció la cuota de ancho de banda requerida por servicio. Las tecnologías que comúnmente se usan en la última milla, como *Frame Relay* y ATM (*Asynchronous Transfer Mode*) poseen el parámetro CIR (*Committed Information Rate*) que equivale al ancho de banda que el suscriptor contrata para tener una transmisión asegurada sin descarte de tramas. En cada sucursal se debe regular la velocidad de envío de los *routers* para que no se exceda el CIR.

Particularmente, la capacidad del enlace de Quito es mayor a la del enlace en Guayaquil. Si las tramas se envían con la máxima velocidad de Quito, es probable que el *buffer* del lado de la sucursal costera se llene y haya descarte de tramas. Por esta razón, es necesario regular la velocidad de envío en Quito para que no se sobrepase la capacidad de Guayaquil.

Como se indicó en el capítulo anterior, se ha considerado el uso del códec G.729 con compresión de cabecera para el ahorro de ancho de banda en el enlace WAN.

3.6 ADMINISTRACIÓN DE LA RED

Para poder llevar el control de los servicios, brindar soporte y resolver conflictos que se puedan producir con el uso de la red, es necesario contar con mecanismos de monitoreo y recopilación de información en los equipos de conectividad y servidores principalmente. Por ello se requieren características como acceso remoto mediante consola, terminales virtuales o WEB y monitorización mediante el protocolo SNMP. También se deben plantear normas básicas de administración, donde intervienen tanto el personal de la empresa como los recursos la red, de manera que se haga uso eficiente de los mismos y se mantenga su alto rendimiento a lo largo del tiempo.

En Telefonía es muy importante llevar el registro exacto de las llamadas y que el usuario tenga consciencia de ello. Para ello se recurrirá al protocolo NTP

(*Network Time Protocol*) que mantendrá sincronizados los teléfonos IP con el servidor de Telefonía IP.

3.6.1 SNMP

La monitorización de los equipos activos como: *switches*, *routers* y servidores es importante para mantener alta disponibilidad dentro de una red detectando oportunamente los incidentes. Para la implementación del servicio de administración de red se plantea el uso del protocolo SNMPv2c (soporte v3 opcional). SNMP es un estándar para la gestión de redes y se encuentra implementado en casi cualquier dispositivo de red imaginado. Todos los dispositivos de conectividad tendrán configurado el protocolo SNMP para ser gestionados mediante las herramientas de administración adecuadas.

Se plantea el siguiente esquema de identificación para las comunidades SNMP: lectura “Adm_alianza_rd”, y escritura “Adm_alianza_wr”.

3.6.2 HERRAMIENTAS DE GESTIÓN

Las herramientas de gestión de red ayudan al Administrador de red a realizar sus actividades de manera más eficiente, rápida y sencilla. Existen herramientas de gestión que permiten monitorear enlaces, dispositivos, equipos de comunicación y servidores.

Para el monitoreo de la red, se privilegiará *software* compatible con la solución de conectividad y Telefonía IP, sea ésta del tipo licenciado o no licenciado. Aunque existen varios *software* de monitoreo completos para dispositivos y enlaces, se recomienda utilizar un *software* que permita más funciones que sólo el monitoreo de la red. Es importante llevar un correcto manejo de licencias e inventario de equipos, por lo que es deseable que la herramienta de gestión también permita realizar estas actividades. Ejemplos de estas herramientas son: *Paessler PRTG Network Monitor*, *What's UP Gold*, *Cacti*, etc. basados en SNMP.

Como herramienta para soporte remoto a los usuarios se seguirá utilizando el programa VNC, por ser un *software* libre y por su bajo consumo de recursos. Es indispensable manejar una redundancia de herramientas para cuando no se pueda acceder a través de la red interna al equipo que necesita soporte. Existen *software* alternativos como *Logmein* y *TeamViewer* que permiten la conexión con el equipo remoto a través de Internet. Si bien son programas licenciados, sus versiones gratuitas limitadas son de mucha utilidad.

3.6.3 POLÍTICAS DE ADMINISTRACIÓN DE RED

Para la administración y gestión de una red no se necesita conocer únicamente el manejo de protocolos y programas de administración de red. También es necesario conocer las actividades que conlleven a incrementar su rendimiento y a que éste se mantenga a lo largo del tiempo. Es importante considerar las siguientes normas de administración:

- Detallar manuales de instalación de programas, *software* y aplicativos.
- Llevar documentación de cableado estructurado con la correspondiente etiquetación del cableado.
- Detallar documentación de red, donde intervengan: direcciones IP de administración de equipos, nombre de usuario y contraseñas para acceso a administración, documentación de las direcciones IP y VLANs.
- Llevar inventarios de *hardware* y *software*.
- Detallar procedimientos a realizarse en caso de falla de algún equipo, pruebas y evaluaciones de diagnósticos de la red.
- Revisar periódicamente los *logs* de servicios.

Entre las constantes actividades relacionadas con la administración de la red, se encuentra la creación de las credenciales de usuarios para acceder a la misma. Para la creación de un usuario de red se plantea la siguiente nomenclatura de acceso:

- Utilización de la primera inicial del nombre unido a su apellido, ejemplo: usuario “Luis Pérez”, nombre de red “lperez”.
- Si existen homónimos se utilizarán las dos primeras letras del nombre unido a su apellido, ejemplo: usuario “Leonardo Perez”, nombre de red “leperez”.

Las buenas prácticas de las actividades a realizar y el buen uso de herramientas de administración red ayudarán a proporcionar un buen servicio de red.

3.6.4 Administración del Cableado Estructurado ^[5]

Para el diseño de la administración del cableado estructurado se considera la norma TIA/EIA 606, donde se establece la información necesaria que se debe presentar para que el sistema de cableado sea administrable.

En este diseño se proponen el registro y etiquetación del sistema de cableado estructurado, el mismo que pretende facilitar la administración. Las etiquetas para las salidas de telecomunicaciones llevarán el indicativo del piso al que pertenecen, si son para voz o para datos y un número de identificación, como en el siguiente ejemplo “SB-D-01”. Esta etiqueta indica que se trata del primer punto de datos, ubicado en el subsuelo. De manera similar se etiquetarán otros elementos como racks, cables, ductos, etc. Los anexos G.1 y G.2 contienen más detalles sobre el registro para la administración del sistema de cableado estructurado.

3.7 SEGURIDAD ^{[58][59]}

El objetivo de los servicios de red es permitir a la empresa manejar tanto su información y la de sus clientes de forma rápida y confiable, sin que ésta se vea comprometida o pueda ser filtrada por cualquier inconveniente o falla de seguridad. Para lograr este cometido, es necesario identificar y separar los servicios vitales para el negocio, como el de bases de datos, de los servicios complementarios, como lo es el servidor de aplicaciones.

Físicamente se deben aislar a estos servicios ubicándolos en equipos diferentes y limitando el acceso físico del personal. El uso de herramientas y equipos de seguridad como el *firewall* y el antivirus ayudan a mitigar posibles ataques. Además, se necesita establecer políticas y reglas relacionadas con el uso y manejo de la información por parte del personal. El objetivo es disminuir puntos de fallo comunes y mejorar la escalabilidad del diseño.

Como precaución contra los posibles ataques internos, se utilizarán ACLs y filtrado de paquetes, reforzados sobre todo en el segmento de red al que se conectan los servidores.

La seguridad en el enlace WAN es una responsabilidad compartida entre el *carrier* y el cliente. El *carrier* provee seguridad básica a través de circuitos virtuales dedicados para el cliente. El cliente en cambio, puede hacer uso de mecanismos de encriptación y VPNs.

3.7.1 FIREWALL Y SISTEMA DE DETECCIÓN DE INSTRUSOS, IDS ^[60]

La seguridad de la información se manejará con un dispositivo *hardware* dedicado a seguridad. Se mantendrá el equipo Kypus como equipo *firewall* y *proxy*. El equipo *firewall* mantendrá su actual configuración y ubicación. Servirá a toda la red corporativa constituida de 200 usuarios aproximadamente y estará ubicado en el núcleo de la red. En la figura 3.12 se puede observar la ubicación del *firewall*. El *firewall* también presentará el servicio de administración de VPN, por ser el dispositivo que hace frente directamente a Internet. No se detalla el funcionamiento de la VPN por estar fuera del alcance de este proyecto.

Si bien el *firewall* previene la mayoría de los ataques externos, éste no analiza los paquetes que llegan a la red, siendo esto una vulnerabilidad. Un mecanismo que cubre parcialmente esta falencia es el IDS (*Intrusion Detection System*). El IDS es básicamente un *sniffer* encargado de analizar los paquetes que entran o salen de

la red y los compara con un grupo de firmas⁹. El equipo Kypus también dispone de IDS, por lo que se procederá a activarlo y configurarlo para prestar sus servicios de seguridad en la red.

3.7.2 SIP TRUNKING SEGURO ^[61]

Con el uso de troncales SIP para el acceso a la PSTN la red corporativa de Alianza de Seguros puede estar expuesta a riesgos que no se tenían con troncales analógicas o digitales. Estos riesgos se deben principalmente a que las troncales SIP usan direcciones IP públicas para su funcionamiento. A pesar de que las troncales SIP funcionan sobre una red IP, éstas no pueden ser protegidas con *firewalls* tradicionales, por lo que la red corporativa podría ser “visible” desde Internet, quedando expuesta a ataques, “hackeo” y otras vulnerabilidades.

Para el acceso seguro a la PSTN mediante troncales SIP se tienen dos opciones: conectar directamente las troncales al servidor de Telefonía, el cual debe tener algún mecanismo de seguridad para troncales SIP, ó conectarlas a un dispositivo de terminación independiente con funciones de controlador de borde de sesiones, SBC (*Session Border Controller*). La mejor práctica es utilizar la segunda opción ya que ofrece seguridad al ocultar la red interna de la red del proveedor de servicios y mejora la interoperabilidad con otros sistemas de Telefonía IP.

3.7.3 POLÍTICAS DE SEGURIDAD DE RED

Las políticas de seguridad dan a conocer a los usuarios la importancia y la sensibilidad de la información. Las políticas de seguridad se detallan como normativas del buen uso y manejo de información. Estas normas determinan procedimientos de manejo de información que deberán cumplir los usuarios.

El objetivo de las políticas de seguridad es brindar confidencialidad, integridad, autenticidad, no repudio, disponibilidad de recursos y de la información,

⁹ Base de datos sobre actividades dañinas de la red.

consistencia, control de accesos y auditoría, para resguardar los recursos y servicios informáticos importantes de la empresa.

3.7.3.1 Análisis de Riesgos de Red

Antes de establecer las políticas de seguridad se debe determinar qué se necesita proteger, de quién y cómo hacerlo, realizando un análisis de riesgos de red.

El primer paso es identificar los recursos a proteger. Los recursos considerados en este caso son: *hardware*, *software*, datos, personal, documentación y accesorios. Estos elementos se muestran en la tabla 3.25.

Recursos	Recursos Específicos
Hardware	<ul style="list-style-type: none"> • Equipos de conectividad como <i>switches</i>, <i>routers</i>, módems, ATAs, etc. • Servidores de datos y Telefonía IP. • Terminales de usuarios como teléfonos, computadoras portátiles, computadoras de escritorio y terminales <i>Thin-Client</i>. • Cableado de red.
Software	<ul style="list-style-type: none"> • Sistemas operativos • Utilitarios • Programas de diagnóstico
Datos	<ul style="list-style-type: none"> • Gestores de datos, como base de datos • <i>Backups</i> • Almacenados en servidores internos y externos
Personal	<ul style="list-style-type: none"> • Usuarios • Operadores de sistemas
Documentación	<ul style="list-style-type: none"> • De red • De <i>hardware</i> • De <i>software</i> • De procedimientos
Accesorios	<ul style="list-style-type: none"> • Información grabada en CDs, DVDs, memorias, discos externos, etc.

Tabla 3.25 *Recursos de Red a proteger*

El segundo paso es identificar de quién se pretende proteger estos recursos, es decir, de personal o *hardware* no autorizados, y de *software* riesgoso o malicioso, lo cual se resume en la tabla 3.26.

De quién proteger?	Detalles
Personal no autorizado	<ul style="list-style-type: none"> • Personas ajenas a la empresa que quieran acceder a ciertos recursos e información. • Usuarios de la red que quieren acceder a información que no son representativas dentro de las actividades que desarrollan. • Personal operativo y de mantenimiento que no se encuentra capacitado para manejar los recursos a proteger.
Software riesgoso o malicioso	<ul style="list-style-type: none"> • Virus • <i>Spyware</i> • <i>Spam</i> • <i>Keyloggers</i>
Hardware	<ul style="list-style-type: none"> • Inclusión de <i>hardware</i> de conectividad ajeno a la empresa sin autorización • Inclusión de terminales de usuario sin autorización

Tabla 3.26 *Resumen de los posibles atacantes de recursos de red*

Finalmente se determina la forma de proteger los recursos que se consideran importantes. Para prevenir riesgos y vulnerabilidades se considera necesario definir las normas de manejo de recursos.

3.7.3.2 Normas del buen uso de recursos de red

3.7.3.2.1 Normativas de acceso

- Todos los equipos de conectividad y servidores se manejarán mediante una contraseña que tendrá letras mayúsculas, minúsculas, números y signos. Esta contraseña será conocida únicamente por el Administrador de red.
- Todos los usuarios que necesiten acceso a algún servicio, deberán llenar un formulario o solicitud del servicio donde se detallen los nombres y apellidos, puesto de trabajo, jefe inmediato, accesos a los servicios de red requeridos y su justificación. La solicitud será realizada por parte del jefe inmediato y dirigida al Administrador de red. El Administrador de red determinará el tipo de cuenta de usuario en base a esta solicitud.

- Las credenciales de usuario serán las únicas válidas para acceder a los recursos. Éstas serán intransferibles, secretas, y de propiedad del usuario.
- Las contraseñas de los usuarios tendrán un tiempo de caducidad mínima de 30 días, la cual deberá ser cambiada por parte del usuario antes de su fecha de caducidad.
- Luego del no uso de una cuenta de usuario por más de 45 días se desactivará. Para su posterior activación, si fuera el caso, se enviará una solicitud al Administrador de red con su respectiva justificación.

3.7.3.2.2 Normativas de seguridad de acceso físico

- Todos los cuartos de equipos y telecomunicaciones estarán asegurados con llave, la misma que estará bajo poder del Administrador de red.
- El acceso a los cuartos de telecomunicaciones y equipos, será responsabilidad del Administrador de red. En caso de requerir que un técnico externo ingrese a los cuartos de telecomunicaciones y equipos deberá ser comunicado al Administrador para que autorice el ingreso.

3.7.3.2.3 Normativas de servicios de red

- El servicio de Internet no deberá ser utilizado para propósitos personales.
- Los usuarios que tengan acceso al servicio de Internet deberán presentar normas de buena conducta.
- Los usuarios de los servicios deberán acatar los principios de integridad y confidencialidad de la información de Alianza de Seguros.
- Los usuarios deben acatar las políticas y normas del servicio
- El usuario debe conocer que el tiempo de respuesta y disponibilidad de los servicios de Internet no pueden ser garantizados al 100%.
- El Departamento de Sistemas se guarda el derecho de control de acceso al servicio de Internet, bloqueando grupos de páginas como: redes sociales, entretenimiento, comercio electrónico, violencia, pornografía y drogas.

- El Departamento de Sistemas se guarda el derecho de bloqueo para los visitantes de páginas WEB que no representen ningún interés comercial para la compañía, entre las que se encuentran: redes sociales, entretenimiento, comercio electrónico, violencia, pornografía y drogas.
- El usuario no debe involucrarse en temas comerciales ajenos a las actividades empresariales o que sean de tipo personal.
- El usuario no debe descargar e imprimir material no relacionado con Alianza de Seguros.
- Se encuentra prohibido el uso de correo electrónico corporativo con fines personales. El usuario es responsable del buen uso de este servicio.
- El usuario no debe enviar archivos con más de 8 MB de tamaño.
- El mensaje enviado será responsabilidad del usuario emisor.
- El usuario debe limitarse a utilizar el espacio determinado para almacenamiento de correos electrónicos en el servidor, que es de 100 MB.
- No se debe emitir mensajes con contenido ofensivo.
- No asumir que los correos luego de enviados siguen siendo privados.
- No utilizar los recursos de red enviando cadenas de correo electrónico.
- No abrir mensajes de remitentes desconocidos.
- No abrir archivos adjuntos sospechosos.
- El usuario es el único responsable de la información que él maneje. En caso de realizar una compartición de archivos, el usuario procederá a brindar la autorización para su acceso.
- El usuario se compromete a utilizar de buena manera el servicio telefónico.
- El Departamento de Sistemas se reserva el derecho de controlar la cantidad de llamadas que un usuario realiza.

3.7.3.2.4 Normativas para el manejo de información

- La información confidencial de la empresa deberá estar encriptada mediante las herramientas proporcionadas por el Departamento de Sistemas.

- Si fuese necesario imprimir información confidencial de la empresa, ésta debe estar etiquetada dentro de una carpeta con el nombre de confidencial y tendrá que ser manejada con mucha precaución. Las carpetas con información confidencial no podrán estar a la vista de todos. El usuario deberá tener esta información bajo llave.
- Los usuarios deben centrarse a manejar información que sólo sea de interés para su área o departamento. Queda prohibido el manejo de información de otros departamentos a menos que ésta sea parte de sus actividades laborales.

3.7.3.2.5 Normativas de software y hardware

- El usuario no deberá instalar *software*, programa o aplicativo sin la previa autorización.
- La instalación de *software* DEMO se la realizará con la colaboración o acompañamiento del proveedor si fuese el caso.
- El *software* y datos obtenidos no deben violar los derechos de propiedad intelectual.
- El uso de cualquier tipo de *hardware* ajeno a la infraestructura tecnológica de Seguros Alianza está restringido. Si fuese necesario su uso se deberá pedir la autorización respectiva al Administrador de red.

3.8 SOLUCIONES DE TELEFONÍA IP

En esta sección se hará la selección del estándar de Telefonía IP entre las opciones SIP y H.323. Se presentarán las directrices mínimas que debe cumplir la solución de Telefonía IP de cada uno de los fabricantes, tradicionales de conectividad como Cisco y HP, y tradicionales de Telefonía como Avaya, para luego detallar cada solución. Finalmente, se hará un análisis comparativo para escoger preliminarmente la ó las soluciones que se adapten mejor a los requerimientos técnicos de la red corporativa de Alianza de Seguros. En el siguiente capítulo se analizarán los costos de la ó las propuestas económicas más sus beneficios, para escoger la solución de Telefonía IP definitiva.

3.8.1 SELECCIÓN DEL ESTÁNDAR PARA TELEFONÍA IP ^{[21][22]}

La Telefonía IP y las comunicaciones unificadas están actualmente regidas por dos estándares: H.323 y SIP. Ambos estándares tienen como finalidad posibilitar las comunicaciones multimedia en tiempo real en redes IP. Sin embargo, estas dos arquitecturas presentan claras diferencias que han ido marcando su evolución y aceptación desde sus inicios hace más de diez años.

De lo analizado en el capítulo uno se ha probado que ambos estándares son lo suficientemente robustos para implementar soluciones concretas de Telefonía IP y comunicaciones multimedia con una amplia gama de servicios.

H.323 tiene una mejor compatibilidad con versiones anteriores. Sin embargo, es un estándar muy rígido que, en aras de proveer todos los servicios necesarios para conferencia multimedia, replica funciones ya disponibles en la red y carece de la flexibilidad necesaria para añadir nuevos servicios y mantener su constante evolución. Con SIP se pueden implementar las mismas y más soluciones que con H.323, además de integrarlas. Adicionalmente, la continuidad y desarrollo en el largo plazo son requisitos primordiales para la selección de cualquier estándar, a lo cual se ajusta de mejor manera el estándar SIP. Debido a esto, SIP se utilizará como el protocolo de control y señalización para este proyecto de Telefonía IP.

3.8.2 DIRECTRICES DE PRESELECCIÓN PARA LA SOLUCIÓN DE TELEFONÍA IP

Entre las marcas que se analizará para escoger la solución de Telefonía IP, existe una gama muy amplia de plataformas para todo tipo y tamaño de necesidad. Por esta razón, se limitará el rango de búsqueda y análisis de cada marca con directrices básicas que cada solución debe cumplir. Los lineamientos se basan en las necesidades empresariales de Alianza y en las características detalladas a lo largo de este capítulo. Las directrices para la solución de Telefonía IP son las siguientes:

- Solución basada en el estándar SIP (RFC 3261).
- Plataforma dedicada para Telefonía IP, tanto en *hardware* como en *software*.
- Plataforma que soporte redundancia.
- Soporte de los códecs G.711 y G.729.
- Plataforma que soporte interacción con la PSTN a través de líneas analógicas, digitales y SIP *trunking* (RFC 2833).
- Solución que soporte las aplicaciones y funciones de Telefonía tradicional.
- Calidad de servicio.
- Soporte para terminales telefónicos IP, analógicos, digitales.
- Soporte para al menos 100 usuarios: fijos, móviles y remotos.
- Soporte para mensajería unificada: integración de fax, correo de voz y correo electrónico convencional, preferentemente con plataforma Linux.
- Soporte para servicios de presencia y mensajería instantánea.
- Soporte para servicios de directorio: integración con *Active Directory* a través de LDAP.
- Soporte de características de administración centralizada. Preferentemente con el protocolo SNMPv2c y consola de administración vía WEB.
- Soporte opcional para implementación futura de características avanzadas como presencia, mensajería instantánea, video, movilidad, IVR, conversión voz/texto, *call center*, etc.

En base a las directrices planteadas, a continuación se presenta una descripción de cada solución, seguida de la selección técnica, donde se presentan los detalles de cada plataforma.

3.8.3 CISCO ^[62]

Entre la gama de productos que Cisco oferta en el área de comunicaciones unificadas, existe una plataforma que se ajusta a las directrices planteadas en la sección anterior, denominada *Unified Communications Manager Business Edition 500 v8.5* (CUCMBE5Kv8.5) basada en SIP y Linux. Esta plataforma de *hardware* y *software* consta de los siguientes elementos principales:

- *Media Convergence Server* MCS-7828-I5
- *Cisco Unified Communications Manager* 8.5 (UCM)
- *Cisco Unity Connection* 8.5 (CUC)
- Terminales telefónicos
- *Routers* como *media gateways*

Los elementos de *software*: *Unified Communications Manager*, *Cisco Unity Connection* y *Unified Presence* normalmente se instalan en un servidor independiente. Sin embargo, gracias a la versión *Business Edition* se pueden integrar a los 2 componentes en un solo servidor. El crecimiento gradual en esta plataforma se da mediante el licenciamiento de los componentes de *software*, terminales telefónicos, y otros elementos que se vayan requiriendo.

3.8.3.1 *Media Convergence Server* MCS-7828-I5 ^{[16][63]}

El servidor convergente MCS-7828-I5 (figura 3.15) es la plataforma de *hardware* primaria que controla las comunicaciones del entorno CUCMBE5Kv8.5. Este servidor cuenta con una arquitectura basada en un procesador *Intel* x3430 *Quad-Core* de 2.4 GHz, 6 GB de memoria RAM tipo DDR3 y dos discos duros SATA de 250 GB con RAID-1. Adicionalmente, tiene dos NIC *Gigabit Ethernet* para la interacción con la red. Esta configuración permite expandir el sistema desde 1 hasta cerca de 500 usuarios con todos los beneficios de comunicaciones unificadas, en apenas 1 unidad de *rack*.

3.8.3.2 *Cisco Unified Communications Manager* 8.5 (UCM) ^{[17][64]}

El *software* servidor UCM es el procesador de llamadas y componente central de la plataforma de comunicaciones unificadas de Cisco basado en Linux. Unifica las aplicaciones de voz, video, datos y movilidad. Es escalable, distribuible y de alta disponibilidad con la implementación de clústeres de servidores. Trabaja con la línea de servidores Cisco MCS. Está basado en el estándar SIP (RFC 3261) tanto para señalización como para el acceso a la PSTN con SIP *trunking* (RFC 2833). Mediante una interfaz WEB se accede a sus funciones de configuración y

administración. Interactúa con terminales SIP de la serie Cisco 7900 y de terceros, entre otros. Se pueden añadir elementos de voz analógicos o digitales a través de *gateways* de voz con estas capacidades. Contiene una consola de administración que se accede vía WEB.



Figura 3.15 Servidor de Telefonía IP Cisco MCS-7828-15

3.8.3.3 Cisco Unity Connection 8.5 (UC) ^[65]

Este componente de *software* integra a la plataforma de comunicaciones unificadas de Cisco con otros servicios de la red. Para mensajería unificada interactúa con servidores y clientes de correo electrónico de otros fabricantes como *MS Exchange*, *IBM Lotus* y *MS Outlook*, a través de protocolos como SMTP e IMAP. *Cisco Unity Connection* es capaz de sincronizar la información de directorio del servicio de Telefonía IP mediante LDAP. Además, incluye funciones avanzadas como el reconocimiento de voz. UC trabaja con los servidores multimedia Cisco de la serie MCS.

3.8.3.4 Terminales Telefónicos ^{[66][67][68]}

Los teléfonos IP de la serie Cisco 7900 (figura 3.16) son compatibles con SIP y poseen las características de voz básicas requeridas, entre ellas el soporte de conferencia multipartita, códecs de voz, *switch* interno de dos puertos, PoE, *display*, teclas programables, etc.

Para las funciones de presencia y mensajería instantánea, Cisco ha introducido el *softphone Unified Personal Communicator 8.0*. Este *softphone* se instala en

cualquier computador con un sistema operativo MS *Windows* XP o superior y combina funciones de video, voz, datos, mensajería instantánea y presencia. Los dispositivos terminales analógicos, como teléfonos o máquinas de fax, se unen a la plataforma de comunicaciones unificadas de Cisco a través de ATAs, como el Cisco ATA 187.



Figura 3.16 *Teléfonos IP Cisco serie 7900*

3.8.3.5 Solución Cisco para Routers como Media Gateways^{[69]-[72]}

Cisco implementa la mayoría de *gateways* de voz en su línea de *routers* para interactuar con la PSTN, entre ellos las series 1900 y 2900. En cada *router* se tiene la opción de añadir tarjetas FXO, FXS, E1, T1, soporte para SIP *trunking* (mediante *Cisco Unified Border Element*), etc. Estos *routers* presentan la función SRST (*Survivable Remote Site Telephony*) que permite al *router* tomar el control de las comunicaciones básicas en ausencia del servidor principal. Adicionalmente, pueden extender sus funciones con el *software* Cisco *Unified Communications Manager Express*.

3.8.4 HP Networking

La plataforma de comunicaciones unificadas más completa de HP es de la serie VCX v7000, basada en SIP y Linux. Abarca *software* para control de comunicaciones o *softphones* como clientes de telefonía IP, y *hardware* para:

servidores, *gateways* de voz y teléfonos. Los elementos principales de esta plataforma son:

- Servidor *HP VCX v7005*
- *Software* de comunicaciones unificadas *VCX 9.5*
- Terminales telefónicos
- *Routers* como *media gateways*.

La plataforma *VCX v7005* crece a medida que se agregan licencias para los diferentes módulos, *software* y dispositivos terminales.

3.8.4.1 Servidor HP VCX v7005 ^{[74][75][76]}

La plataforma *VCX v7005* tiene como base un servidor *HP Proliant 120 DL G6*. En este servidor viene un procesador *Intel Xeon X3430*, 2 GB de memoria RAM tipo *DDR3* y un disco duro *SATA* de 250 GB. Consta de 2 puertos *RJ-45 Gigabit Ethernet* para el acceso a la red. Dependiendo de la versión del *software* que se instale, esta configuración puede soportar desde decenas hasta cerca de 500 usuarios. Este servidor ocupa una unidad de *rack*.

3.8.4.2 Software de Comunicaciones Unificadas VCX 9.5 ^{[77][78]}

En la plataforma *VCX v7000* las funciones de comunicaciones unificadas se manejan a través del *software VCX 9.5*. El *software VCX 9.5* está basado en una plataforma endurecida de *Linux* y en el estándar *SIP RFC 3261*. Tiene varios modos de configuración, siendo el más completo el de “Servidor de Telefonía IP y Mensajería”. Este modo se encarga del procesamiento de las llamadas, lleva el registro de *CDRs*, controla las características de administración y servicios de directorio, etc. La integración con otros servicios de red los hace a través de protocolos como *SMTP* e *IMAP* para correo electrónico, *T.38* para fax, *LDAP* para el directorio, entre otros. Entre dos servidores *VCX v7005* existe la posibilidad de hacerlos trabajar en conjuntos dentro de esquemas de alta disponibilidad con

redundancia y balanceo de carga. La consola de administración de esta plataforma se accede vía WEB.

3.8.4.3 Terminales Telefónicos y Gateways de Voz ^{[79][80]}

La plataforma VCX v7000 acepta teléfonos IP de la serie HP 3500 y HP 3100, con soporte SIP, y el *softphone* HP VCX Desktop Communicator Software. Los teléfonos de la serie 3500 y 3100 soportan los estándares PoE, conferencia, *switch* interno de dos puertos, etc. Con el *softphone* HP VCX Desktop Communicator Outlook Edition Software se pueden acceder a las funciones avanzadas de mensajería instantánea e integración con MS Outlook.

Los terminales analógicos se pueden conectar a través de *gateways* de voz de la serie V7111.

La figura 3.17 muestra un ejemplo de los teléfonos IP compatibles con la plataforma VCX.



Figura 3.17 Teléfonos IP HP serie 3500 y 3100. Servidor HP VCX v7005

3.8.4.4 Solución HP para Routers como Media Gateways ^{[81][82][83]}

Las sucursales que requieren menor capacidad que un servidor, o no necesitan todas sus prestaciones, hacen uso de los *routers* HP de la serie A-MSR-30 compatibles con la plataforma VCX. Estos *routers* permiten que las llamadas de la sucursal puedan ser re-enrutadas a la PSTN en caso de pérdida de la conexión con el servidor principal. Se puede extender sus funciones con la adición del

módulo *HP VCX Enterprise Branch Communications MIM*, para que se comporte como un servidor de Telefonía IP con el *software VCX*.

Una falencia de la plataforma VCX es que no soporta troncales SIP de forma nativa. Para su implementación se necesita un equipo compatible de terceros, aprobado por los laboratorios HP. En este caso se tiene la opción del módulo *HP VCX IP Telecom Module x3250M2, SIParator*, de la marca Ingate.

3.8.5 AVAYA ^{[84][85]}

La plataforma para empresas medianas de *Avaya* se llama *IP Office R7.0*. Ésta incluye los elementos de comunicaciones unificadas esenciales, como funciones de voz, mensajería unificada y movilidad. *Avaya IP Office R7.0* tiene soporte SIP y se compone de los siguientes elementos principales:

- *IP Office control unit 500v2*
- *IP Office Manager*
- *VoiceMail Pro*
- Terminales telefónicos

El crecimiento de esta plataforma se da al añadir unidades de control *IP Office 500*, tarjetas y las licencias del caso. Para el soporte de servicios avanzados como la presencia mediante SIMPLE, se requieren otros elementos de *Avaya*, como *SIP Enablement Services*.

3.8.5.1 *IP Office Control Unit 500v2* ^{[86][87]}

IP Office control unit 500v2 es el *hardware* principal de procesamiento de llamadas, conexión de dispositivos terminales y circuitos troncales de la PSTN. Todas estas funciones se implementan a través de la combinación de 4 tarjetas internas, ya sean de extensión o módulos de compresión de voz, y distintos módulos de expansión para terminales y troncales analógicos y digitales. Las características de terminales SIP, fax T.38 y troncales SIP se soportan mediante

los módulos de compresión de voz. Este equipo viene en presentación para montura de *rack* de 19" y puede expandir sus funciones con la adición de otras unidades de control 500v2. Una sola unidad de control puede dar servicio hasta 384 extensiones. La figura 3.18 muestra el panel frontal y posterior del equipo *IP Office control unit 500v2*. El panel posterior contiene dos puertos RJ-45 para la conexión a la red.

La unidad de control *IP Office 500* viene con el *firmware IP Office 7.0* propietario de Avaya.

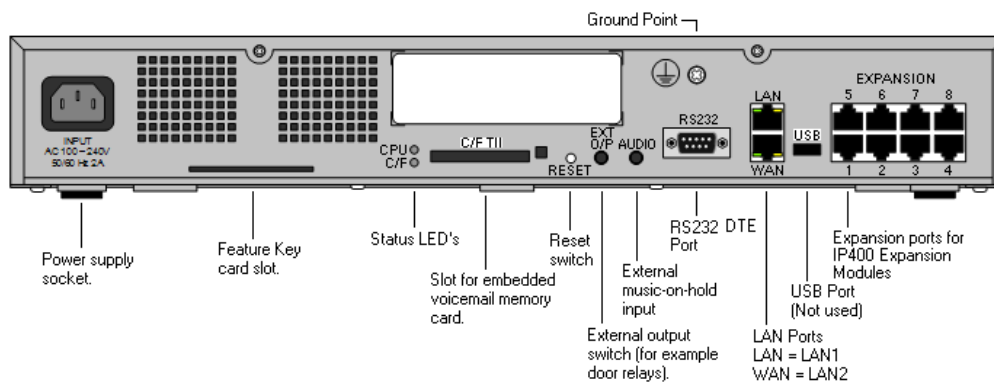


Figura 3.18 Avaya *IP Office control unit 500v2*. Vista posterior

3.8.5.2 *IP Office Manager 9.0* ^[87]

El *software IP Office Manager 9.0* tiene la función de facilitar la instalación, configuración y administración de la unidad de control *IP Office 500*. Es una aplicación que requiere un computador compatible con *Microsoft Windows XP* o superior para su instalación y uso. Permite administrar varias unidades de control *IP Office 500* conectados en un esquema distribuido. También incluye el *software* de monitoreo *System Monitor*, como aplicación independiente.

3.8.5.3 *VoiceMail Pro* ^[84]

Las opciones de mensajería unificada de *Avaya IP Office* se implementan con el *software VoiceMail Pro*. *VoiceMail Pro* provee al servicio telefónico de buzón de correo. La integración con otras plataformas de correo, como *MS Exchange 2007*,

requiere del componente de mensajería unificada UMS (*Unified Messaging Service*). A pesar de que existe una versión para *MS Windows* y otra para Linux, las características de integración con productos como *MS Outlook* necesitan la versión de *MS Windows*. Soporta SMTP para integración con otros sistemas de mensajería.

3.8.5.4 Terminales Telefónicos ^{[88][89][90]}

Los teléfonos IP Avaya de la serie 9600 son compatibles con SIP y con la plataforma *IP Office 500*. Entre sus características principales están las teclas programables, soporte de PoE, *switch* interno de dos puertos, *display*, etc. Los terminales analógicos se pueden conectar directamente al sistema *IP Office 500*, siempre y cuando se instalen las tarjetas para extensiones analógicas.

Los usuarios remotos interactúan con *IP Office* a través del *softphone IP Office*, el cual se instala en un computador basado en *MS Windows XP* o superior.

3.8.6 ANÁLISIS Y SELECCIÓN DE LA SOLUCIÓN DE TELEFONÍA IP

Los elementos descritos en cada una de las soluciones anteriores cumplen con las directrices básicas de selección. Sin embargo, para escoger la mejor opción técnica entre las diferentes plataformas, en el anexo L.2 se detallan y comparan las características básicas de Telefonía IP, tales como las versiones de los estándares, protocolos y productos de *software* soportados, el *hardware* necesario, además de los mecanismos de crecimiento, redundancia, calidad de servicio, administración, seguridad y licenciamiento, acordes al diseño de red propuesto en este capítulo y a la reducción de costos. También se indican los requerimientos adicionales de *software* y/o *hardware* para las características que no se incluyen dentro de cada una de las soluciones. Estos requerimientos pueden estar incluidos en otras plataformas del mismo fabricante o en plataformas de terceros. A continuación se plantea la mejor solución técnica de Telefonía IP, en base a los lineamientos anteriores.

Según las comparaciones de requerimientos del anexo L.2, la plataforma que cumple de mejor manera con las especificaciones técnicas es: *Cisco Unified Communications Manager Business Edition 5000 v8.5*, de Cisco. Esta plataforma supera a las demás, en características como: el soporte de todas las versiones de SNMP (la única que incluye la versión requerida v2c), integración con la mayoría de versiones del cliente de correo electrónico *MS Outlook* y del servicio de directorio *MS Active Directory*, mecanismos de seguridad y soporte para troncales SIP. Todas las características básicas obligatorias se soportan con la menor cantidad de *hardware* y *software* posibles del mismo fabricante: un servidor de Telefonía IP en Quito y dos *routers* para la funciones de *gateway* y terminación de troncales SIP, tanto para Quito como para Guayaquil; *software* de control CUCM y mensajería unificada CUC, además de los teléfonos IP y *softphones*.

Como se planteó en la sección de seguridad, la plataforma de Cisco también admite que un dispositivo independiente sea el punto de terminación para las troncales SIP mediante CUBE, además del servidor de Telefonía IP. CUBE puede ser implementado en un equipo dedicado, o como se plantea en diseño, junto con el *gateway*, para el ahorro de costos.

Las características avanzadas opcionales de implementación futura también se favorecen con la plataforma de Cisco. El soporte de video, movilidad, presencia y mensajería instantánea puede incluirse en la plataforma CUCMBE5Kv8.5, por lo que sólo se necesitan el *hardware* del servidor, los terminales telefónicos adecuados (ej: *softphones*) y la red inalámbrica para su despliegue. El soporte explícito para la base de datos DB2 de IBM, así como las características de IVR y *call center*, únicamente requiere un servidor adicional, centralizado o distribuido, con el *software* Cisco CCX 8.0.

La marca Cisco suele tener un costo elevado y complejos métodos de licenciamiento. Sin embargo, la plataforma CUCMBE5Kv8.5 cuenta con esquemas de licenciamiento que unifican todos sus componentes (usuarios, puertos, terminales de usuario, costos de uso, etc.) en paquetes únicos basados en el número de usuarios a soportar (ver anexo L.2, sección Licenciamiento y

Soporte). Con este esquema de licenciamiento y la reducida cantidad de equipos y *software* necesarios, se disminuye la complejidad del sistema y el costo total a corto y largo plazo.

3.9 RESUMEN DE REQUERIMIENTOS DE MATERIALES Y EQUIPOS

El anexo L contiene el resumen de los requerimientos de materiales y equipos de conectividad para la reingeniería de la red corporativa, como se explica a continuación:

- **Anexo L.1.** Materiales para el cableado estructurado.
- **Anexo L.2.** Matriz de comparación de requerimientos de la plataforma para Telefonía IP.
- **Anexo L.3.** Requerimientos para *switches*. Se incluye el cumplimiento de estos requerimientos con equipos de la marca Cisco por su confiabilidad, por compatibilidad con los equipos de Telefonía IP seleccionados y por las ventajas de administrar una red homogénea.
- **Anexo L.4.** Requerimientos para servidores de antivirus, *Thin-Client*, correo electrónico y archivos.
- **Anexo L.5.** Requerimientos para teléfonos IP. Se incluye el cumplimiento de estos requerimientos para equipos de la marca Cisco, por ser la plataforma de Telefonía IP seleccionada.

El resumen de los requerimientos permitirá obtener las cotizaciones respectivas de los proveedores y verificar su cumplimiento.

3.9.1 EQUIPOS DE CONECTIVIDAD REUTILIZABLES

Los equipos de conectividad actuales de la empresa tienen características básicas que sirvieron para solucionar los problemas conforme éstos se han presentado, por lo que se necesita determinar qué equipos pueden ser

reutilizados. Con la tabla 3.27 se verifica si alguno de los *switches* existentes en Alianza de Seguros cumple con los requerimientos mínimos del diseño.

Los requerimientos mínimos planteados son los de un *switch* de acceso. Dos de las características más importantes en esta capa son las de administración y PoE. Excepto por el *switch* 3COM 4200, ninguno de los otros *switches* cumple con la característica de administración. Aunque no cumple con el requerimiento de PoE, cumple con los requerimientos básicos para servir de respaldo en la capa de distribución de la ciudad de Quito. Las especificaciones detalladas del *switch* 3COM 4200 se adjuntan en el anexo M.

Características mínimas requeridas para <i>switches</i> de Acceso									
Marca	Modelo	10/100 Mbps	QoS	PoE	VLAN	Store& Forward	Adm*	Auto-sense	STP
3Com	4200	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí
3Com	2016	Sí	Sí	No	No	Sí	No	Sí	Sí
D-Link	1024R+	Sí	No	No	No	Sí	No	Sí	No
Encore	ENH905-NWY	Sí	No	No	No	Sí	No	Sí	No
TrendNet	TE100-S5TE100S5	Sí	No	No	No	Sí	No	Sí	No
Linksys	SD208	Sí	No	No	No	Sí	No	Sí	No
CNET	CSH-800	Sí	No	No	No	Sí	No	Sí	No
TP-LINK **	TL-SG1024	Sí. Hasta1000 Mbps	No	No	No	Sí	No	Sí	No

* *Switch* con capacidades de administración

** *Switch* de Guayaquil Centro

Tabla 3.27 *Condiciones para los switches de posible reutilización*

En Guayaquil se cambiarán todos los *switches* ya que no cumplen las características mínimas necesarias para su reutilización.

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 3

LIBROS

- [1] EDWARDS James, BRAMANTE Richard. "Networking Self-Teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management and Maintenance". Primera Edición. Edit. John Wiley & Sons. 2009.
- [2] SOSINSKY Barrie. "Networking Bible". Primera Edición. Edit. Wiley Publishing. 2009.
- [3] ANSI/TIA/EIA. "ANSI/TIA/EIA-568-B.1-2001". Edit. Telecommunications Industry Association. 2001
- [4] ANSI/TIA/EIA. "ANSI/TIA/EIA-569-A TIA/EIA TELECOMMUNICATIONS SYSTEMS BULLETIN: Transmission Performance Specifications for Field Testing of Unshielded Twisted-Pair Cabling Systems". Edit. Telecommunications Industry Association. 1995
- [5] ANSI/TIA/EIA. "ANSI/TIA/EIA-606 Administration Standard for Commercial Telecommunications Infrastructure". Edit. Telecommunications Industry Association. 2002
- [6] ZIKOPOULOS Paul C. "DB2® Version 8: The Official Guide". Primera Edición. Edit. Prentice Hall PTR. 2003.
- [7] LEVINE John. "qmail". Primera Edición. Edit. O'Reilly. 2004
- [8] HUNTER Laura E., ALLEN Robbie. "*Active Directory Cookbook*". Tercera Edición. Edit. O'Reilly. 2008
- [9] CARTER Gerald. "LDAP System Administration". Primera Edición. Edit. O'Reilly. 2003
- [10] WALLINGFORD Theodore. "Switching to VoIP". Primera edición. Edit. O'Reilly. 2005
- [11] BAYER Michael. "Computer Telephony Demystified - Putting CTI, Media Services, and IP Telephony to Work". Primera Edición. Edit. McGraw-Hill Professional. 2000.

- [12] YARBERRY William A. "Computer Telephony Integration". Segunda Edición. Edit. Auerbach Publications. 2003.
- [13] MADSEN Leif, VAN MEGGELEN Jim, & SMITH Jared. "Asterisk: The Definitive Guide". Tercera Edición. Edit. O'Reilly. 2011.
- [14] HANES David, SALGUEIRO Gonzalo. "Fax, Modem and Text for IP Telephony". Primera Edición. Edit. Cisco Press. 2008.
- [15] SAINT-ANDRE Peter. "XMPP: The Definitive Guide". Primera Edición. Edit. O'Reilly. 2009.
- [16] PILTZECKER Anthony. "How to cheat at administering Office Communications Server 2007". Edit. Syngress Publishing Inc. 2007
- [17] RITTINGHOUSE John W., RANSOME James F. "Instant Messaging Security". Primera Edición. Edit. Elsevier Digital Press. 2005.
- [18] MORGAN Brian. "Cisco Unified Presence Fundamentals". Primera Edición. Edit. Cisco Press. 2010.
- [19] KENYON Tony. "Data Networks: Routing, Security, and Performance Optimization". Primera Edición. Edit. Digital Press. 2002
- [20] DAVIDSON Johnathan. "Voice over IP Fundamentals". Segunda Edición. Edit. Cisco Press. 2006.
- [21] AHSON A. Syed, ILYAS Mohammad. "SIP Handbook: services, technologies, and security of the Session Initiation Protocol". Primera Edición. Editorial CRC Press. 2009
- [22] KAZA Ramesh. "Cisco IP Telephony: Planning, Design, Implementation, Operation, and Optimization". Primera Edición. Edit. Cisco Press. 2005

PROYECTOS DE TITULACIÓN

- [23] BONILLA Jorge, CARRASCO Daniel. "Análisis e implementación de un prototipo de servidor virtualizado sobre una distribución de Linux para el uso en pymes". Quito, Febrero 2010. Pag 288-308

INTERNET

- [24] <http://zeuz-dc.blogspot.com/2008/08/normas-t568at568b.html>
- [25] ANSI/EIA/EIA-607 (CSA T527)
<http://www.ense.be/PDF/2040.pdf>
- [26] <http://networkcable-tester.com/2011/03/09/patch-panel-3/>
- [27] <http://www.lindy.co.uk/lindyshop/pictures/60572big.jpg>
- [28] <http://www.dintekelectronic.com/lan/components>
- [29] <http://esp.hyperlinesystems.com/img/sharedimg/jacks/pl-rj45-c6.jpg>
- [30] http://www.mercadolibre.com.ec/jm/img?s=MEC&f=8717261_3563.jpg&v=O
- [31] Plenum (CMP) Vs. Riser (CMR) Cable Types for Cat 5 and Cat 6 (para el tema del tipo de cable CMP vs CMR)
<http://www.lanshack.com/pdf/PlenumVsRiser.pdf>
- [32] http://www.cisco.com/en/US/products/hw/modules/ps4999/products_tech_note09186a00807a30d6.shtml#model
- [33] http://www.n-tron.com/pdf/network_availability.pdf
- [34] <http://www.faqs.org/rfcs/rfc2453.html>
- [35] DB2 Version 9 for Linux, UNIX, and *Windows*
<http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.apdv.cli.doc/doc/t0024242.htm>
- [36] http://www.sendmail.com/sm/open_source/download/
- [37] <http://cr.yip.to/qmail.html>
- [38] Step by Step Installation of a Secure Linux Web, DNS and Mail Server
http://www.sans.org/reading_room/whitepapers/linux/step-step-installation-secure-linux-WEB-dns-mail-server_1372
- [39] qmail
<http://cr.yip.to/qmail.html>
- [40] <http://technet.microsoft.com/es-es/windowsserver/bb414778>
- [41] <http://www.reciclemos.net/docs/pdfs/Manual%20de%20clientes%20livianos.pdf>
- [42] http://www.mcafee.com/mx/enterprise/products/system_security/servers/virusscan_enterprise.html
- [43] <http://technet.microsoft.com/es-es/windowsserver/bb414778>
- [44] <http://www.centos.org/>

- [45] <http://technet.Microsoft.com/es-es/Windowsserver/bb414778>
- [46] http://es.wikipedia.org/wiki/Windows_Server_2008
- [47] http://www.onyougo.es/hp-vcx-v7111-je366aabb-puntos-de-acceso_pi293453
- [48] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps514/ps11026/data_sheet_c78-608596.pdf
- [49] http://www.cisco.com/warp/public/cc/so/neso/bbssp/poeie_wp.pdf
- [50] http://www.poweroverethernet.com/articles.php?article_id=52
- [51] http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/troubleshooting/power_over_ethernet.html
- [52] <http://rep.mgeups.com/edg/edg/technote/kw.pdf>
- [53] <http://www.newark.com/pdfs/techarticles/hoffman/airConditioners-sizingSelection.pdf>
- [54] <http://www.kooltronic.com/dg-h-e-select-man.php>
- [55] Configuration Guidelines for DiffServ Service Classes
<http://www.ietf.org/rfc/rfc4594.txt>
- [56] http://www.cisco.com/en/US/products/hw/modules/ps4999/products_tech_note09186a00807a30d6.shtml#model
- [57] WAN QoS
<http://www.cisco.com/en/US/docs/video/cuvc/design/guides/srnd/vidqos.html>
- [58] <http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad>
- [59] <http://www.xbackup.net/spanish/PoliticadeseuridaddeRed>
- [60] <http://upcommons.upc.edu/pfc/bitstream/2099.1/3451/9/52096-9.pdf>
- [61] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/gatecont/ps5640/white_paper_c11-620461.pdf
- [62] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7273/data_sheet_c78-587917.pdf
- [63] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/data_sheet_c78-635855.pdf
- [64] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps556/data_sheet_c78-652908.pdf

- [65] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps6509/data_sheet_c78-634096.pdf
- [66] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps10326/IP_Phones_Positioning_External_December2009.pdf
- [67] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps6836/ps6844/data_sheet_c78-609335.pdf
- [68] <http://www.cisco.com/en/US/products/ps5853/index.html>
- [69] <http://www.cisco.com/en/US/products/ps5854/index.html>
- [70] http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf
- [71] <http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html>
- [72] http://www.cisco.com/en/US/prod/collateral/routers/ps10537/data_sheet_c78_553896.pdf
- [73] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps2169/data_sheet_c78-570481.pdf
- [74] http://h17007.www1.hp.com/us/en/products/unified-communications/HP_VCX_V7000_Unified_Communications_Series/index.aspx
- [75] http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02735917/c02735917.pdf?jumpid=reg_R1002_USEN
- [76] http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02735917/c02735917.pdf?jumpid=reg_R1002_USEN
- [77] <http://www.dectrader.com/docs/set5/c02735961.pdf>
- [78] http://h17007.www1.hp.com/us/en/products/unified-communications/HP_350x_IP_Phone_Series/index.aspx
- [79] http://h17007.www1.hp.com/us/en/products/unified-communications/HP_310x_IP_Phone_Series/index.aspx
- [80] http://h17007.www1.hp.com/docs/products/eos/End-of-Sale-Announcement-for-VCX-IP-Telecommuting-Module-JE404A_v4.pdf
- [81] <http://pdfs.icecat.biz/pdf/26966199-4310.pdf>
- [82] www.arp.com/medias/pdf/MIME094158.pdf
- [83] <http://support.avaya.com/css/P8/documents/100130188>

- [84] http://pm-v3.stage.globalworks.com/rt/default.aspx?CurrentPath=emea/en-us/products/offers/sip_enablement_services.htm&Wrapper=Print&View=ProdPrint
- [85] <http://www.ipofficeinfo.com/TechBulletins/tb135.pdf>
- [86] http://badgercommunications.com/pdf/avaya/1-manager_en.pdf
- [87] <http://www.avaya.com/es/resource/assets/brochures/lb3473se.pdf>
- [88] http://www.kingdomcommunicationstexas.com/Avaya_9600_Series_IP_Deskp_hones_-_Brochure.pdf
- [89] <http://www.its.am/pdf/Phone%20Manager.pdf>
- [90] http://www.n-tron.com/pdf/network_availability.pdf

CAPÍTULO 4

ANÁLISIS DE COSTOS

En el presente capítulo se realiza un análisis de costos para la inversión de la reingeniería de la red para la Compañía de Seguros y Reaseguros Alianza S.A. Se analizarán los costos para los elementos pasivos y activos de la red corporativa. Al final del capítulo se analizan las perspectivas de recuperación de la inversión para el tiempo de vida estimado del proyecto.

El valor del IVA (Impuesto al Valor Agregado) del 12% se deberá incluir en el costo total del proyecto, donde constan todos los componentes para la red corporativa. Todos los valores se encuentran cotizados en dólares de los Estados Unidos de América (USD).

4.1 COSTO DE LA RED PASIVA

Los costos de la red pasiva abarcan todos materiales, instalación y certificación del cableado estructurado para Quito (tabla 4.1). Los materiales para el cableado estructurado son de las marcas Quest y Dexson. El precio referencial de cada uno de los elementos a utilizar y su instalación fue provisto por la empresa NETCATEL y se detallan en el anexo N.1.

4.2 COSTO DE LA RED ACTIVA

Dentro de los costos de la red activa se analizarán los costos de las soluciones de Telefonía IP, conectividad, servidores redimensionados y enlaces WAN. En esta sección también se detallan los diferentes equipos a utilizar, más las condiciones de soporte, mantenimiento y garantía para equipos, además de los respectivos costos de instalación.

ITEM	PRECIO FINAL
Materiales	\$ 12.829,95
Instalación 152 puntos de red categoría 6	\$ 4.712,00
Certificación 152 puntos de red categoría 6	\$ 760,00
Instalación racks y accesorios	\$ 1.500,00
TOTAL	\$ 19.801,95

Tabla 4.1 Costo total del Sistema de Cableado Estructurado

4.2.1 SOLUCIÓN DE TELEFONÍA IP

En el capítulo anterior se determinó que la solución de Telefonía IP que cumple con todos los requerimientos técnicos para este proyecto es la plataforma de Cisco: *Unified Communications Manager Business Edition 5000 v8.5*, CUCMBE5Kv8.5. Esta es la plataforma de Telefonía IP para la cual se procederá con el desglose y análisis de costos. Se hará énfasis en los beneficios que la solución de Cisco aporta al diseño de la red y al costo total de la inversión, a corto y mediano plazo.

Los costos para la solución de Telefonía IP se desglosarán en: *hardware* y *software*; licencias, instalación, soporte y mantenimiento. La proforma económica ha sido provista por la empresa ANDEAN-TRADE y se incluye en el anexo N.2.

4.2.1.1 *Hardware y software* ^{[3]-[7]}

Los precios mostrados en la tabla 4.2 incluyen al servidor de Telefonía IP, teléfonos IP gerenciales, de gama media y de recepción, *softphone*, ATAs y *gateways*. Los precios que se muestran en la tabla 4.2 incluyen los accesorios y tarjetas adicionales que requieren todos los equipos.

La plataforma de Cisco requiere *hardware* y *software* para brindar los servicios de Telefonía IP. El servidor MCS-7828 (figura 4.1) viene pre cargado con los elementos de *software Cisco Unified Communications Manager v8.5* y *Cisco Unity*

Connection v8.5. El primero se encarga del control de las comunicaciones y el segundo de la mensajería unificada, como se detalló en el capítulo 3. Estos elementos de *software* normalmente se distribuyen e instalan en servidores independientes; no obstante, la plataforma CUCMBE es la única donde se encuentra a esos dos elementos en el mismo servidor. Esto representa una importante ventaja frente a otras plataformas ya que se ahorran costos, espacio físico y recursos en la administración; todo esto soportado por la redundancia en almacenamiento con RAID y la alta confiabilidad del servidor MCS7828 cuyo MTBF supera las 30000 horas.

CÓDIGO	DESCRIPCIÓN	CANT.	PRECIO UNITARIO	PRECIO FINAL
Servidor de Telefonía IP				
MCS7828I5-K9-WL8	Servidor Principal de Telefonía IP, incluye 50 primeros usuarios	1	\$ 12.916,20	\$ 12.916,20
Teléfonos y ATAs				
CP-7942G	Teléfono IP gerencial. Incluye adaptador y cable de poder.	11	\$ 306,07	\$ 3.366,77
CP-7911G	Teléfono IP gama media. Incluye adaptador y cable de poder.	67	\$ 213,25	\$ 14.287,62
CP-7962G	Teléfono IP recepción. Incluye adaptador y cable de poder.	2	\$ 377,47	\$ 754,94
CP-7915=	Botonera teléfono recepción	2	\$ 342,72	\$ 685,44
ATA187-I1-A=	ATA para teléfonos analógicos y faxes	6	\$ 228,48	\$ 1.370,88
UPC8-K9-PC	<i>Softphone</i>	1	\$ 0,00	\$ 0,00
Gateway Quito				
C2901-VSEC-CUBE/K9	Gateway de voz, SIP <i>trunking</i> para 25 sesiones. Incluye 1 tarjeta PVDM3-16 y 2 tarjetas VIC2-4FXO	1	\$ 5.392,20	\$ 5.392,20
Gateway Guayaquil				
C2901-VSEC-CUBE/K9	Gateway de voz, SIP <i>trunking</i> para 25 sesiones. Incluye 1 tarjeta PVDM3-16 y 2 tarjetas VIC2-4FXO	1	\$ 5.392,20	\$ 5.392,20
TOTAL				\$ 44.166,25

Tabla 4.2 *Costos de equipos de Telefonía IP*

Cisco distribuye el servidor de comunicaciones unificadas más el *software* como un paquete, denominado MCS7828I5-K9-WL8. Las especificaciones técnicas de la

plataforma CUCMBE5Kv8.5, del servidor MCS7828 y de los elementos de *software* de la plataforma se encuentran en los anexos O.1, O.2, O.3 y O.4.

Los teléfonos de la serie Cisco 7900 son compatibles con SIP e incluyen todas las características previstas en el capítulo 3 (ver anexo L.5). Se han seleccionado los teléfonos 7942G, 7911G y 7962G para gerentes, personal regular y recepcionistas respectivamente. Los teléfonos 7942G y 7962G cuentan con una amplia pantalla (figura 4.2) donde se despliega la información de las llamadas entrantes, las líneas telefónicas en uso (2 y 6 respectivamente), fecha y hora, directorio telefónico, etc. Adicionalmente, sus teclas pre programadas sirven de acceso rápido a los mensajes de voz y directorio telefónico. Por otro lado, los teléfonos de la serie 7911G, tienen una pantalla reducida y soportan sólo 1 línea telefónica. Particularmente, el teléfono 7962G puede trabajar en conjunto con el módulo de expansión Cisco 7915, para ampliar el número de líneas y extensiones a manejar.



Figura 4.1 *Servidor Cisco MCS 7828*



Figura 4.2 *Teléfono IP Cisco 7942G. Pantalla de los teléfonos IP Cisco 7942G y 7962G*

Debido a que cada ATA187 soporta dos dispositivos analógicos (figura 4.3), se han cotizado 3 para Quito y 3 para Guayaquil, de tal manera que se tienen 6 puertos FXS en cada localidad.

Se ha considerado que los *gateways* de voz, que sirven de complemento para la plataforma de comunicaciones unificadas de Cisco, sean implementados mediante *routers* Cisco 2901 (figura 4.4), por las siguientes razones:

- **Compatibilidad con la plataforma CUCMBE5Kv8.5.** Los *routers* Cisco 2901 llevan una imagen del *software Cisco Unified Communications Manager Express*, CUCME, que es compatible con la plataforma de comunicaciones unificadas seleccionada.
- **Supervivencia local.** Los *routers* Cisco 2901 admiten el uso de SRST, mecanismo de Cisco para evitar la pérdida del servicio telefónico local en caso de que el servidor de Telefonía IP o la comunicación con él fallen.
- **SIP *trunking*.** El mismo *router* 2901, donde reside la imagen de CUCME y SRST puede contener a su vez la imagen del *software* CUBE para el manejo de las troncales SIP. Gracias a esto, la terminación de las troncales SIP es ajena al servidor de Telefonía IP, con lo que se tiene la mayor seguridad en el acceso a los servicios de la PSTN.
- **Modularidad.** El *router* Cisco 2901 soporta varias tarjetas para las troncales analógicas de respaldo con puertos FXO. También admite módulos para el procesamiento de voz adicionales al que ya contiene, y otras tarjetas para puertos FXS, E1, etc.

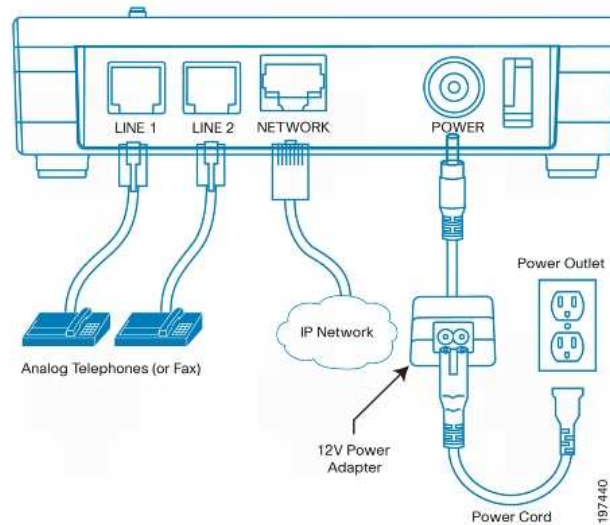


Figura 4.3 Vista posterior de Cisco ATA187 y dispositivos compatibles

Cada uno de estos *routers* también incluyen:

- 1 tarjeta PVDM3-16 para procesar 16 canales de voz adicionales, además de la tarjeta PVDM3-16 que viene integrada.
- 2 tarjetas VIC2-4FXO para las líneas troncales analógicas de respaldo y de fax.

Como se puede apreciar, la plataforma de Cisco permite brindar todas las funciones requeridas para el *gateway* de voz, con mayor disponibilidad, seguridad, y menor cantidad de equipos, tal como se planteó en el capítulo anterior, en la sección de diseño de red.



Figura 4.4 Router Cisco 2901. Vistas frontal y posterior

Los anexos O.5, O.6 y O.7 contienen las especificaciones técnicas de los teléfonos Cisco 7942G, 7911G y 7962G, y el anexo O.8, las especificaciones para el *router* Cisco 2901.

4.2.1.2 Licencias ^[8]

A excepción de la plataforma de comunicaciones unificadas CUCMBE de Cisco, las plataformas HP VCX 7005 y Avaya IP Office R7.0 requieren una licencia específica para cada tipo de teléfono, usuario, programa informático, troncal, etc.

La plataforma CUCMBE5Kv8.5 trabaja con el esquema de licencias *Cisco Unified Communications Manager Business Edition Workspace Bundle*. Este esquema de licencias por usuario incluye: el uso del servidor MCS7828 y los *software*: *Cisco Unified Communications Manager 8.5*, *Cisco Unity Connection 8.5*, *Cisco Unified Presence 8.5*, *Cisco Unified Personal Communicator 8.5*, *Cisco Unified IP Communicator* con *Cisco Unified Video Advantage*, entre otros. También se incluyen las licencias de integración con otras plataformas de comunicaciones unificadas, mediante *Cisco Unity Connection*, así como las licencias para usuarios avanzados y teléfonos IP. Como se puede apreciar, este esquema de licencias contempla adicionalmente las opciones de movilidad, video y presencia.

Particularmente, el paquete MCS7828I5-K9-WL8 incluye las licencias para los primeros 50 usuarios con todas las características de Telefonía IP descritas anteriormente. A partir del usuario número 51 se requiere la compra de licencias individuales. En este proyecto se requiere licencias para 83 usuarios en total con todas las características necesarias; por lo tanto, además de las 50 licencias que vienen con el paquete inicial, se deben adquirir 33 licencias adicionales, las cuales se muestran la tabla 4.3.

LICENCIA	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO FINAL
MCS7828I5-K9-WL8	Servidor con paquete inicial, incluye licencias para 50 primeros usuarios con todas las prestaciones	1	\$ 0,00	\$ 0,00
CUCM-BE-WL	Licencia para un usuario CUCMBE	33	\$ 239,40	\$ 7.900,20

	con todas las prestaciones			
C2901-VSEC-CUBE/K9	Gateway con paquete inicial, incluye las licencias CUBE para manejar 25 troncales SIP	2	\$ 0,00	\$ 0,00
ANLG-DEV-BE	Licencia para terminal analógico	10	\$ 38,00	\$ 380,00
FL-CME-SRST-25	Licencias SRST para 25 teléfonos IP	1	\$ 418,00	\$ 418,00
FL-CME-SRST-25	Licencias SRST para 5 teléfonos IP	3	\$ 114,00	\$ 342,00
TOTAL				\$ 9.040,20

Tabla 4.3 Costos de Licencias para Telefonía IP

Para disminuir costos, los terminales telefónicos analógicos tienen licencias especiales por una fracción del costo de una licencia regular. Las funciones avanzadas, como el uso de troncales SIP o la sobrevivencia local SRST, no se incluyen con el paquete inicial del servidor y tienen licencias independientes que deben ser adquiridas por separado. Los *routers* 2901 que se cotizaron traen pre cargado consigo el *software* CUBE para el manejo de 25 troncales SIP cada uno, lo cual cubre el número de troncales SIP requeridas con una ligera holgura. A estos *routers* se les debe agregar las licencias del *software* SRST para la supervivencia local. Se utilizará SRST para la cerca de la mitad de teléfonos en cada localidad, por lo que se requerirán licencias SRST para 25 teléfonos IP en Quito y para 15 teléfonos IP en Guayaquil. La tabla 4.3 muestra todas las licencias requeridas para el sistema completo de Telefonía IP.

4.2.1.3 Condiciones de Soporte y Mantenimiento Anual ^[9]

El principal contrato de mantenimiento que ofrece Cisco es SMARTnet. SMARTnet cuenta con soporte técnico telefónico gratuito de fábrica y reemplazo de partes y piezas al siguiente día laborable como máximo; además incluye las actualizaciones de *software* completamente gratis. Este contrato tiene duración de 1 año, pero puede ser renovado al término del mismo. Por otro lado, el servidor de Telefonía IP MCS7828 no cuenta con SMARTnet, sino con el contrato de mantenimiento especial CON-ECPM-MCS78281 que cubre el soporte para reemplazo de *hardware*, actualizaciones de *software* y tiene la opción de visitas

técnicas en las instalaciones del cliente. En la tabla 4.4 se pueden observar los costos por el servicio de soporte.

SERVICIO	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO ANUAL	PRECIO FINAL
CON-ECPM-MCS78281	Soporte para el servidor de Telefonía IP	1	\$ 1.403,14	\$ 1.403,14
CON-SNT-CP7942G	Soporte teléfono IP 7942G	11	\$ 159,00	\$ 1.749,00
CON-SNT-CP7911G	Soporte teléfono IP 7911G	67	\$ 39,00	\$ 2.613,00
CON-SNT-CP7962G	Soporte teléfono IP 7962G	2	\$ 159,00	\$ 318,00
CON-SNT-CP7915	Soporte módulo de expansión 7915	2	\$ 159,00	\$ 318,00
CON-SNT-ATA18711	Soporte ATA 187	6	\$ 39,00	\$ 234,00
CON-SNTP-2901CMST	Soporte Router 2901	2	\$ 549,00	\$ 1098,00
			TOTAL	\$7.733,14

Tabla 4.4 Costos de Soporte y Mantenimiento de Telefonía IP

4.2.1.4 Garantía, Instalación y Costo Total de la Solución de Telefonía IP ^{[10][11][12]}

Las garantías del equipo servidor de Telefonía IP, *gateways* y teléfonos tienen validez de 1 año. En caso de daño del equipo por los motivos especificados en la garantía del mismo, éste puede ser remplazado según las normativas del contrato de soporte, donde se especifica que se remplazará el equipo en un periodo no mayor a 10 días. AndeanTrade prestará el servicio de instalación tanto para Quito como para Guayaquil. El costo total de la solución de Telefonía IP se detalla en la tabla 4.5.

COMPONENTE	PRECIO FINAL
Equipos	\$ 44.166,25
Licencias	\$ 9.040,20
Soporte	\$ 7.733,14
Instalación	\$ 7.600,00
TOTAL	\$ 68.539,59

Tabla 4.5 Costos total de la plataforma de Telefonía IP CUCMBE5Kv8.5

Se debe tomar en cuenta que con la plataforma de Cisco la implementación de opciones avanzadas como presencia, video, movilidad, IVR y *call center* se hacen

con la adición de la menor cantidad posible de *hardware* y *software* si se la compara con las soluciones Avaya IP Office o HP VCX 7005. El servicio de presencia requiere únicamente el *hardware* del servidor, ya que el *software* está incluido en la presente propuesta. Las características de video se pueden activar con el uso de terminales telefónicos adecuados (ej: *Cisco Unified Personal Communicator*). El IVR y el *call center* se activan mediante un servidor con el *software Cisco Unified Contact Center 8.0* que incluye el soporte para la base de datos DB-2 de IBM.

4.2.2 SOLUCIÓN DE CONECTIVIDAD

En el capítulo anterior se hizo una selección previa de los equipos de conectividad en base a los requerimientos técnicos. Se han escogido equipos de la marca Cisco, preferibles por su compatibilidad con la solución de Telefonía IP, su confiabilidad, la homogenización de la red, facilidades de administración, etc. Además, se presentan como anexos propuestas económicas con equipos equivalentes de las marcas HP y D-Link por motivos de comparación. La propuesta con equipos HP tiene un costo superior a la de equipos Cisco, mientras que la de equipos D-Link tiene un costo inferior, pero sus equipos tienen una confiabilidad menor en comparación a los de Cisco. En los anexos N.3, N.4, N.5 se incluyen los precios referenciales para los equipos de conectividad para las marcas Cisco, D-Link y HP respectivamente. Por las razones citadas, el análisis de costos sólo se realizará con la marca Cisco.

4.2.2.1 Equipos de Conectividad ^{[13]-[21]}

Los *switches* están divididos por capas:

- Acceso: *switches* Cisco WS-C2960-24PC-S y WS-C2960-48PST-S (figura 4.5) de 24 y 48 puertos respectivamente con PoE.
- Distribución: *switches* Cisco WS-C2960G-24TC-L de 24 puertos (figura 4.6).

- Núcleo: dos *switches* Cisco WS-C3560G-24TS-S (figura 4.7) de 24 puertos, uno para Quito y uno para Guayaquil.



Figura 4.5 *Switches de acceso Cisco WS-C2960-24PC-S y WS-C2960-48PST-S*



Figura 4.6 *Switch de distribución Cisco WS-C2960G-24TC-L*



Figura 4.7 *Switch de núcleo Cisco WS-C3560G-24TS-S*

Las características principales para los *switches* C3560G y C2960G son el soporte de puertos *Giga Ethernet*, ACLs y que pueden expandir sus capacidades al uso de fibra óptica. Por otra parte, los *switches* C2960 de 24 y 48 puertos cuentan con puertos *Fast Ethernet* para el acceso y suministran PoE. El *switch* WS-C2960-24PC-S tiene la capacidad de suministrar PoE en todos sus puertos, mientras que el *switch* WS-C2960-48PST-S sólo en la mitad de ellos. Todos los *switches* manejan calidad de servicio. El *switch* de núcleo tiene funciones de capa 3 para el enrutamiento entre VLANs.

En la tabla 4.6 se presentan los precios relativos a los equipos de conectividad Cisco

EQUIPO	DESCRIPCIÓN	CANT.	PRECIO UNITARIO	PRECIO FINAL
WS-C2960-48PST-S	SWITCH CATALYST 2960 48 10/100 PoE + 2 1000BT + 2 SFP LAN <i>Lite</i> Image	4	\$ 2.352,20	\$ 9.408,80
WS-C2960-24PC-S	SWITCH CATALYST 2960 24 10/100 PoE + 2 T/SFP LAN <i>Lite</i> Image	3	\$ 1.364,20	\$ 4.092,60
WS-C2960G-24TC-L	SWITCH CATALYST 2960 24 10/100/1000, 4 T/SFP LAN Base Image	2	\$ 2.504,20	\$ 5.008,40
WS-C3560G-24TS-S	SWITCH CATALYST 3560 24 10/100/1000T + 4 SFP + IPB Image	2	\$ 3.626,22	\$ 7.252,44
PWR-RPS2300	<i>Fuente Cisco Redundant Power System 2300 and Blower, No Power Supply</i>	2	\$ 907,50	\$ 1815,00
CAB-RPS2300=	<i>Cable de poder para fuente Spare RPS2300 Cable for Devices other than E-Series Switches</i>	2	\$ 113,44	\$ 226,88
TOTAL				\$ 27.804,12

Tabla 4.6 Costo de switches marca Cisco

4.2.2.2 Soporte y Mantenimiento Anual^[22]

Los equipos marca Cisco cuentan con el soporte SMARTnet de 8 horas al día en 5 días a la semana. El soporte responde por fallas en el *hardware* con la posibilidad de cambio del equipo en 4 horas y visita del personal técnico en las instalaciones del cliente. Este servicio se renueva anualmente e incluye acceso a las últimas versiones de *software* para sus equipos. Los rubros para el soporte se encuentran en la tabla 4.7.

4.2.2.3 Instalación, Garantía y Costo Total de la Solución de Conectividad

La propuesta de la empresa AndeanTrade cubre también los costos de instalación y configuración básicas de los equipos para las localidades de Quito y Guayaquil. La garantía es válida por un año y cubre defectos de fábrica. Estos costos se muestran en la tabla 4.8 junto con el costo total de la propuesta.

SERVICIO	DESCRIPCIÓN	CANT.	PRECIO UNITARIO	PRECIO FINAL
CON-SNTE-2964STL	SMARTNET 8X5 4HR SVC 48 PORT PoE 370W 1 año	4	\$ 241,21	\$ 964,84
CON-SNTE-C29602PC	SMARTNET 8X5X4 CAT 2960 24 10/100 PoE 2T/SFP LAN BSE IM 1 año	3	\$ 194,32	\$ 582,96
CON-SNTE-C2960G2C	SMARTNET 8X5 4HR CAT SVC 2960 24 10/100/1000 1 año	2	\$ 374,31	\$ 748,62
CON-SNTE-3560GTS	SMARTNET 8X5X4 CAT 3560 24 10/100/1000T + 4 SFP St 1 año	2	\$ 576,92	\$ 1.153,84
TOTAL				\$ 3.450,26

Tabla 4.7 Costo del soporte para switches marca Cisco

COMPONENTE	PRECIO
Equipos	\$ 27.804,12
Soporte	\$ 3.450,26
Instalación	\$ 2.500,00
TOTAL	\$ 33.754,38

Tabla 4.8 Costo total de la solución de conectividad

4.3 SERVICIO DE TRANSPORTE DE DATOS

Los costos de servicio de transporte de datos se cotizaron en base a los requerimientos técnicos obtenidos en el dimensionamiento de los enlaces WAN en el capítulo 3. Se solicitó una propuesta económica al proveedor de servicios de telecomunicaciones TELCONET, que es el proveedor actual del servicio para Alianza de Seguros, gracias a una alianza estratégica con Megadatos S.A. Se prefirió a este proveedor por la confianza que Alianza de Seguros tiene en sus servicios. La empresa TELCONET detalló en su propuesta los costos por enlace, los acuerdos de servicio y operación, más la garantía.

4.3.1 COSTOS DE ENLACES ^[23]

El proveedor de servicios TELCONET cuenta con núcleo y *backbone* urbano con tecnología MPLS, tal como se requiere. TELCONET realizó la propuesta

contenida en el anexo N.6 y mostrada en la tabla 4.9 para el cubrimiento de los requerimientos de conectividad WAN.

Punto A	Punto B	Servicio	AB [kbps]	Medio transmisión	Instalación	Precio mensual
Quito	Quito	Internet	4096	Fibra óptica	\$ 150,00	\$ 640,00
Quito	Gye – centro	Tunel IP	1536	Fibra óptica	\$ 150,00	\$ 450,00
Quito	Gye Kennedy	Tunel IP	512	Fibra óptica	\$ 150,00	\$ 370,00
Quito	Machala	Tunel IP	256	Fibra óptica	\$ 150,00	\$ 310,00
Quito	Milagro	Tunel IP	512	Fibra óptica	\$ 150,00	\$ 370,00
Quito	Cuenca	Tunel IP	1024	Radio	\$ 150,00	\$ 410,00
Quito	Manta	Tunel IP	512	Fibra óptica	\$ 150,00	\$ 370,00
Quito	Santo Domingo	Tunel IP	512	Fibra óptica	\$ 150,00	\$ 255,00
Subtotal					\$ 1.200,00	\$ 3.175,00
TOTAL						\$ 4.375,00

Tabla 4.9 *Cotización de enlaces WAN e Internet*

Es importante mencionar que el servicio de datos tiene un costo mensual recurrente, mientras que la instalación tiene un costo no recurrente. Se menciona también que el proveedor en su oferta emite un contrato de servicio de 12 meses de duración con un tiempo de instalación de máximo 15 días. Para el proceso de instalación el cliente debe hacerse cargo de las obras civiles y la obtención de los permisos para el montaje de la infraestructura requerida.

4.3.2 ACUERDOS DE SERVICIO Y OPERACIÓN ^[24]

La propuesta emitida por el proveedor incluye los siguientes acuerdos de servicio y operación:

- Enlaces dedicados con compartición 1:1
- Garantiza un nivel de servicio de 99.8%
- Retardo de circuito internacional de 120 ms

- Retardo de circuito nacional de 9 ms
- Retardo de circuito local de 1 ms
- Pérdida de paquetes cercanos al 0%
- Tiempo promedio de reparación (MTTR, por sus siglas en inglés) de 2 horas
- Soporte técnico 24x7x365

4.4 TRONCALES SIP

Las troncales SIP serán provistas por la Corporación Nacional de Telecomunicaciones, CNT. La pensión básica mensual del número de troncales es por paquete. Los paquetes son de 5, 10, 20 o 30 troncales. Se escogerá un paquete de 10 y uno de 5 troncales para completar las 15 troncales necesarias de Quito, y un paquete de 20 troncales para cubrir las 19 troncales necesarias de Guayaquil. Los precios de las troncales han sido obtenidos mediante asesores comerciales de la CNT y de su página WEB. Los costos de instalación y pensión básica mensual de las troncales SIP se muestran en la tabla 4.10. Los precios referenciales se adjuntan en el anexo N.7.

ITEM	CANTIDAD	PRECIO UNITARIO	PRECIO FINAL
Pensión Básica Mensual			
5 canales SIP, 10 números asignados, 192 kbps	1	\$ 60,00	\$ 60,00
10 canales SIP, 20 números asignados, 384 kbps	1	\$ 120,00	\$ 120,00
20 canales SIP, 40 números asignados, 640 kbps	1	\$ 240,00	\$ 240,00
Troncal analógica comercial	8	\$ 12,00	\$ 96,00
Subtotal			\$ 516,00
Derechos de inscripción e instalación			
Troncal SIP 5 canales	1	\$ 300,00	\$ 300,00
Troncal SIP 10 canales	1	\$ 600,00	\$ 600,00
Troncal SIP 20 canales	1	\$ 1.200,00	\$ 1.200,00
Troncal analógica comercial	8	\$ 60,00	\$ 480,00
Subtotal			\$ 2580,00
TOTAL			\$ 3.096,00

Tabla 4.10 *Costos por Troncales Telefónicas SIP y Respaldo*

4.5 SERVIDORES ^{[25][26][27]}

Los servidores serán de la marca *HP Proliant*, serie DL360G7 E5640 (figura 4.8) con sistema operativo *Microsoft Windows 2008 Server*. La cotización provista por la empresa Binaria-Sistemas se adjunta en el anexo N.8. Los costos para los servidores se resumen en la tabla 4.11. Las especificaciones técnicas del servidor HP Proliant DL360G7 se detallan en el anexo O.9.

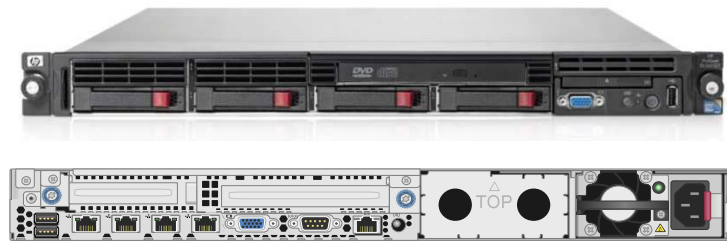


Figura 4.8 *Servidor HP Proliant DL360G7. Vistas Frontal y Posterior*

4.6 PERSPECTIVAS DE RETORNO DE LA INVERSIÓN ^{[1][2]}

A continuación se evalúa el retorno de la inversión, para lo cual se analizan los ingresos, los costos de inversión, operación y mantenimiento. Para finalizar, se realiza el flujo de fondos para determinar los costos durante el tiempo de vida del proyecto.

4.6.1 INGRESOS

Para este proyecto, se definen a los ingresos como aquellos rubros que se reducirán o no se desembolsarán por concepto de mantenimiento, compra de equipos nuevos para la red o el ahorro económico por el uso de la Telefonía IP y reducción de troncales IP. El rubro más importante es el ahorro de costos por consumo telefónico.

Los rubros de ahorro por reducción de gastos de mantenimiento y compras de equipos nuevos para telefonía y conectividad se los obtuvo del presupuesto anual del Departamento de Sistemas de la empresa.

ITEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO FINAL
Hardware				
HP Proliant DL360G7 E5640	Servidor HP DL360G7 Procesador Intel E5640, RAM 6 GB HDD 146 GB RAID-1, 460 w,1 HU	3	\$ 3.721,18	\$ 11.163,54
Software				
WinSvrStd 2008R2 SNGL OLP NL	Microsoft Windows Server 2008	1	\$ 740,68	\$ 740,68
WinSvrCAL 2008 SNGL OLP NL UsrCAL	Licencias para Microsoft Windows Server 2008	4	\$ 29,84	\$ 119,36
Soporte				
HP 3y 4h 24x7 ProLiant DL36x HW Support	Soporte HP 24x7 para <i>hardware</i> de servidores por 3 años	3	\$ 450,40	\$ 1.351,20
TOTAL				\$ 13.374,78

Tabla 4.11 *Costos de Hardware, Software y Soporte para Servidores*

Como se estableció en el diseño, se pretende colocar troncales SIP, con lo que se reducen a 8 las troncales analógicas que se emplearán para respaldo y líneas de fax, tanto en Quito como Guayaquil. Actualmente, entre Quito y Guayaquil se tienen 49 troncales analógicas, de las que se pretende eliminar 33. Conociendo que el costo de la pensión básica mensual por troncal analógica es de \$ 12, sin IVA, se tendrá un ahorro anual de \$ 4752.

Para el análisis del ahorro de costos, se debe tomar en cuenta que las llamadas entre Quito y Guayaquil ya no cruzarán por la red de la CNT, con el ahorro respectivo. Con el análisis telefónico realizado en el capítulo 2, se encontró que desde Quito hacia Guayaquil se hacen 23 llamadas, y desde Guayaquil hacia Quito se realizan 44 llamadas, con un promedio de duración de 220 y 240 segundos respectivamente. El costo por minuto de una llamada comercial nacional es de \$ 0,063, incluido IVA.

CONSUMO TELEFÓNICO						
Origen-destino de las llamadas	# Llamadas diarias	Días laborales por mes	Duración llamada [min]	Costo de llamada por minuto	Ahorro mensual	Ahorro anual
Quito-Guayaquil	23	20	3,67	\$ 0,056	\$ 94,45	\$ 1.133,44
Guayaquil-Quito	44	20	4,00	\$ 0,056	\$ 197,12	\$ 2.365,44
Ahorro por consumo telefónico						\$ 3.498,88
PENSIÓN BÁSICA						
Localidad	# troncales analógicas actuales	# troncales analógicas luego de la reingeniería	# troncales analógicas a eliminar	Pensión básica mensual	Ahorro mensual	Ahorro anual
Quito	27	8	19	\$ 12,00	\$ 228,00	\$ 2.736,00
Guayaquil	22	8	14	\$ 12,00	\$ 168,00	\$ 2.016,00
Ahorro por pensión básica						\$ 4.752,00
Subtotal ahorro (ahorro por consume telefónico + ahorro por pensión básica)						\$ 8.250,88
IVA ahorrado 12%						\$ 990,11
AHORRO TOTAL ANUAL						\$ 9.240,99

Tabla 4.12 *Ahorro anual por eliminación de troncales y consumo telefónico*

En la tabla 4.12 se detalla el número de llamadas mensuales considerando que el mes tiene 20 días laborables. Además, en el cálculo de la pensión básica se considera el IVA. En esta tabla se muestra también el ahorro anual aproximado que se va a tener con el desarrollo del proyecto.

Además de los beneficios en administración, seguridad, productividad, entre otros, que representa la reingeniería de la red con servicios de Telefonía IP, el ahorro anual aproximado directo por reducción de consumo telefónico y troncales, será de \$ 9.240,99, mostrado en la tabla 4.12. Adicionalmente, entre las ventajas de la Telefonía IP, se encuentra el control de las llamadas que realizan los empleados. Esto permitirá reducir los costos por las llamadas que no sean de interés o productividad propios de la empresa, con lo que se espera reducir aún más el consumo telefónico.

4.6.2 COSTOS DE INVERSIÓN

Los costos de inversión representan todos aquellos valores que se pagan una sola vez al inicio del proyecto. Estos costos incluyen los nuevos equipos (*hardware* y *software*), partes pasivas que componen la red y la instalación de estos elementos. El desglose de los costos de inversión se muestra en la tabla 4.13.

COMPONENTE	PRECIO FINAL
Cableado Estructurado	\$ 19.801,95
Telefonía IP	\$ 68.539,59
Conectividad	\$ 33.754,38
Transporte de Datos	\$ 1.200,00
Troncales Telefónicas (SIP y analógicas)	\$ 2.580,00
Servidores (<i>hardware</i> y <i>software</i>)	\$ 13.374,77
Subtotal	\$ 139.250,69
IVA 12%	\$ 16.710,08
TOTAL	\$ 155.960,77

Tabla 4.13 *Costos totales de inversión del proyecto*

4.6.3 COSTOS DE OPERACIÓN Y MANTENIMIENTO

Los costos de operación y mantenimiento de la red son gastos recurrentes. Se incluye el soporte y mantenimiento anual de los equipos, así como las mensualidades de enlaces WAN y troncales telefónicas. El costo total de operación y mantenimiento anual se presenta en la tabla 4.14.

DESCRIPCIÓN	PRECIO FINAL
Soporte técnico equipos de Telefonía IP	\$ 7.733,14
Soporte técnico equipos de conectividad	\$ 3.450,26
Costo anual de arrendamiento de enlaces	\$ 38.100,00
Costo básico anual de troncales analógicas y SIP	\$ 6.192,00

Soporte técnico de servidores (<i>hardware</i>)	\$ 350,44
SUBTOTAL	\$ 55.825,84
IVA	\$ 6.699,10
TOTAL	\$ 62,524.94

Tabla 4.14 *Costos totales de operación y mantenimiento del proyecto*

4.6.4 FLUJO DE FONDOS^{[1][2][28]}

Para el análisis de flujos de fondos se determinan las siguientes consideraciones:

- Un horizonte de evaluación de cinco años y un costo de oportunidad del 10%.
- Que los gastos de Operación y Mantenimiento son fijos y no incrementales dentro de los cinco años de análisis del proyecto.
- Que los ingresos tendrán un valor incremental anual del 5%.
- La depreciación que tendrán los equipos a adquirir y la depreciación del cableado estructurado. El cableado estructurado no se considera como un activo fijo, pero tampoco un equipo electrónico, por lo que su depreciación se realiza para los 5 años de duración del proyecto (ver tabla 4.16).

4.6.5 RENTABILIDAD^{[1][2][28][29]}

La rentabilidad del proyecto será evaluada mediante el valor actual neto, VAN. Este valor se ha obtenido mediante las fórmulas de cálculo de *Microsoft Excel* en base a los valores de la tabla 4.17. La tasa interna de retorno TIR no se puede evaluar ya que no se presenta al menos un flujo positivo para el periodo previsto. En la tabla 4.15 se muestra el índice de rentabilidad generado.

ÍNDICE	VALOR
VAN	-\$ 248.667,70

Tabla 4.15 *Índice de rentabilidad VAN*

De lo mostrado en las tablas 4.16 y 4.17, se determina un índice de rentabilidad negativo, es decir, que si bien la reingeniería de la red corporativa para Alianza de Seguros con inclusión de servicios de Telefonía IP no retornará el total de la inversión en el periodo analizado de 5 años, se tienen importantes ingresos con el ahorro del consumo telefónico. A esto deben sumarse los beneficios en administración, seguridad, productividad y competitividad que generará esta tecnología para la empresa. Se espera que, con la nueva infraestructura de red propuesta en este proyecto, los ingresos de la empresa se incrementen considerablemente, ya que aumentará la eficiencia del personal y se podrá atender a un mayor número de clientes en menor tiempo; aunque la inversión tecnológica inicial aparente ser costosa.

El cálculo del beneficio económico que Alianza de Seguros percibiría por la reingeniería de su red está fuera del alcance de este proyecto. En este cálculo se deberían tomar en cuenta los múltiples factores y variables que afectan los ingresos y egresos de la compañía, para determinar el beneficio económico real.

DEPRECIACIÓN									
Valor	Tiempo de** depreciación [años]	Depreciación anual	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	
\$ 44.166,25	3	\$14.574,86		\$14.574,86	\$ 4.574,86	\$ 14.574,86			
\$ 11.163,54	3	\$ 3.683,97		\$ 3.683,97	\$ 3.683,97	\$ 3.683,97			
\$ 27.804,12	3	\$ 9.175,36		\$ 9.175,36	\$ 9.175,36	\$ 9.175,36			
\$ 12.829,95	10	\$ 1.283,00		\$ 1.283,00	\$ 1.283,00	\$ 1.283,00	\$ 1.283,00	\$ 1.283,00	
		TOTAL DEPRECIACIÓN		\$ 28.717,19	\$28.717,19	\$ 28.717,19	\$ 1.283,00	\$ 1.283,00	\$ 1.283,00

* Sólo se toman en cuenta los activos tangibles, en este caso sólo *hardware*.

** Se considera que el *hardware* se deprecia en 3 años, mientras que el cableado estructurado, en 10 años, por su tiempo de vida.

Tabla 4.16 Depreciación de los equipos presentados en la solución

FLUJO DE FONDOS
Ingresos por reducción de pago de consumo a CNT
Ingreso por reducción de líneas troncales
Ingreso por reducción de equipos
Ingresos por gastos de mantenimiento telefonía tradicional
Ingreso por reducción de equipos de conectividad
Ingresos por gastos de mantenimiento equipos de
TOTAL INGRESOS
DEPRECIACIÓN
GASTOS DE O&M
UTILIDAD NETA
+ 35.4% IMPUESTOS
TOTAL
COSTO TOTAL INVERSIÓN
DEPRECIACIÓN
FLUJO DE FONDOS NETO PURO

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 4

LIBROS

- [1] CASCO Eduardo, “Apuntes de Evaluación de Proyectos”. Quito, EPN, 2009

PROYECTOS DE TITULACIÓN

- [2] BOLAÑOS Emilio. “Diseño de la red inalámbrica de área local para los edificios la Tribuna y Villafuerte de Petroproducción bajo el estándar IEEE 802.11g y su interconectividad”. Quito, Septiembre 2008. Pag 206-215

INTERNET

- [3] http://cisco.biz/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps7273/data_sheet_c78-636588.pdf
- [4] <http://content.etilize.com/Large/1013388645.jpg>
- [5] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps8535/product_data_sheet0900aecd8069bb68.html
- [6] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps514/ps11026/data_sheet_c78-608596.html
- [7] <http://img.alibaba.com/wsphoto/v0/342790034/New-Sealed-Cisco-2901-Integrated-Services-Router-CISCO2901-K9.jpg>

- [8] <http://media.gswi.westcon.com/media/Website%20OneX/website%202010/Cisco%20Workspace%20Licensing%20-%20At%20a%20Glance.pdf>
- [9] http://www.cisco.com/web/LA/productos/servicios/docs/services_data_sheet_spa.pdf
- [10] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/data_sheet_c78-635855.pdf
- [11] http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/phones/ps379/ps6565/prod_qas0900aecd8039de5e.html
- [12] http://www.cisco.com/web/LA/productos/servicios/docs/services_data_sheet_spa.pdf
- [13] http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd806b0bd8.pdf
- [14] http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/product_data_sheet0900aecd80322c0c.pdf
- [15] http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5528/product_data_sheet09186a00801f3d7d.pdf
- [16] http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_55_se/configuration/guide/2960scg.pdf
- [17] http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.1_19_ea1/configuration/guide/3560SCG.pdf
- [18] <http://www.getprice.com.au/images/uploadimg/BimgCisco%20WS-C2960-24PC-S.jpg>
- [19] <http://www.netoby.com/sites/default/files/imagecache/Preview900/WS-C2960-48PS.jpg>
- [20] http://img.alibaba.com/img/pb/290/828/315/315828290_836.jpg
- [21] <http://www.router-switch.com/ws-c3560g-24ts-s-p-475.html>
- [22] http://www.cisco.com/en/US/prod/cisco_serv_to_warranty_comp_0509.pdf
- [23] <http://www.telconet.net/?lang=es§ion=solutions&content=03>
- [24] <http://www.telconet.net/?lang=es§ion=solutions&content=01>
- [25] http://www.cnt.gob.ec/index.php?option=com_content&view=article&id=93:linuevresi&catid=29:prodtelefonija?Itemid=27
- [26] <http://content.etilize.com/Original/1019288399.jpg>
- [27] <http://www.visiocafe.com/downloads/hp/HP-ProLiant.zip>

- [28] Conceptos de evaluación de proyectos
http://www.eco-finanzas.com/economia/evaluacion_de_proyectos.htm
- [29] Conceptos de VAN y TIR
<http://www.elblogsalmon.com/conceptos-de-economia/que-son-el-van-y-el-tir>
- [30] Cálculo del VAN y TIR en Excel
<http://www.zonaeconomica.com/excel/van-tir?page=4>

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el mercado nacional el cable UTP tipo CMP o *plenum* es escaso. Esto se debe a su elevado costo que, dependiendo de la marca, puede hasta cuadruplicar el precio de su contraparte, el cable UTP tipo CMR o *riser*. Sin embargo, el cable CMP tiene un recubrimiento especial que retarda la propagación del fuego en caso de incendios y emite gases menos tóxicos. En caso de incendio gracias a estas características el personal del edificio tendría más tiempo para la evacuación, aspirar menos gases nocivos y así salvar su vida. Ésta es la razón de su elevado precio. El cable CMP debe emplearse en instalaciones donde existan corrientes de aire, como el cielo raso u otros espacios abiertos. Los códigos de construcción nacional deberían promover su utilización frente al cable CMR.
- Con el análisis de la red corporativa se pudo constatar el uso de malas prácticas de crecimiento y escalabilidad debidas al desconocimiento. El criterio más utilizado para la escalabilidad de las redes es aumentar el ancho de banda en los puertos de los *switches*. Sin embargo, esta medida

resulta no ser tan acertada si no va de la mano de otras características que impidan la saturación de la red. Esto se evidencia con la existencia de numerosos *switches* de bajo precio con capacidad *Gigabit* en cada puerto. No obstante, muchos de ellos no soportan la carga total en todos sus puertos y con ello deterioran el rendimiento global de las redes de las que forman parte.

- Uno de los elementos más importantes dentro de la red es la infraestructura de cableado estructurado. Aunque este componente es muchas veces subestimado, resulta ser una de las principales causas de caída de los servicios de red en caso de avería. Por esta razón, es menester seguir las normas de diseño de cableado estructurado que garantizan el mejor desempeño de la red pasiva, así como su adecuada y permanente administración.
- Los sistemas privados de Telefonía tradicional se caracterizaban por su escasa interoperabilidad entre equipos de diferentes marcas, lo que obligaba a los usuarios a utilizar únicamente los equipos y accesorios de un fabricante determinado. Esta tendencia se va venciendo con Telefonía IP y la influencia de las redes de datos. Sin embargo, aún quedan rezagos del esquema propietario, y aunque la Telefonía IP esté basada en estándares abiertos como SIP o H.323, se debe verificar la interoperabilidad entre equipos de distintas marcas antes de adquirirlos.
- Las ventajas de la Telefonía IP sobre la Telefonía tradicional sobresalen cuando se tiene una organización empresarial distribuida, como es el caso de Alianza de Seguros. En Telefonía tradicional el esquema más común era tener una centralita en cada localidad, propia de la empresa, para administrar y brindar el servicio a nivel local. Para la interconexión de las localidades remotas, era necesario hacer uso de los servicios de la PSTN y su costo en función del consumo. Con el objetivo de reducir costos, la Telefonía IP da la posibilidad de utilizar una sola central IP en una localidad específica y controlar terminales remotos ya sea directamente, o a través

de algún dispositivo intermedio, como lo son los *gateways*. Para la interconexión entre la central IP y los terminales remotos es necesario únicamente un enlace IP y el ancho de banda suficiente para las llamadas. Este enlace suele tener un costo mensual fijo.

- En el presente trabajo se ha rediseñado la red corporativa de la empresa Alianza de Seguros para que la infraestructura pueda enfrentar los desafíos tecnológicos actuales. Además, se sienta la base para soportar el crecimiento de la infraestructura y el advenimiento de nuevos servicios, según las necesidades de la empresa.
- El diseño de una red con calidad de servicio se basa en dar un trato preferencial y diferenciado al tráfico que lo requiere. En el sitio más alto de prioridad se encuentra el tráfico de voz. Esto se debe principalmente a la percepción del receptor, el oído humano. Éste requiere que la llegada de los paquetes de voz sea fluida para que los mensajes puedan ser interpretados correctamente. Para ello, se deben tomar medidas en cada uno de los elementos que intervienen en la comunicación, desde los terminales telefónicos, pasando por *switches* y *routers* para conseguir calidad de servicio fin-a-fin.
- El diseño de red propuesto, prevé una etapa de transición entre los servicios de Telefonía tradicional y los servicios de Telefonía IP puros. Es por esta razón que se conservan temporalmente varios equipos y servicios tradicionales, como teléfonos analógicos, máquinas de fax, líneas troncales analógicas, etc. De esta manera usuarios y clientes tienen tiempo de adaptarse a la nueva tecnología sin abandonar sus hábitos comunes de la noche a la mañana. Después de la transición, estos elementos pueden ser desechados sin afectar en lo más mínimo el funcionamiento del servicio o de la red.

- Los días en que la calidad de la voz en Telefonía IP tenía que equipararse a la calidad percibida en la PSTN están llegando a su fin. El límite de los 4 puntos en la escala MOS conseguidos con los 64 kbps del códec más conocido, G.711, está siendo superado por los nuevos códecs de banda ancha. Códecs como el G.722, denominados de alta definición, pueden trabajar con el mismo ancho de banda, pero entregan una calidad auditiva más fiel gracias a la ampliación de la frecuencia de muestreo. Con estos códecs los terminales telefónicos requieren micrófonos y altavoces diseñados específicamente para audio de alta definición.
- Con la incorporación de la Telefonía IP a los servicios de la red aparecen también otros desafíos que deben enfrentarse. Uno de ellos es la seguridad de la red corporativa en el acceso a los servicios de la PSTN a través de troncales SIP. Dado que los *firewalls* tradicionales no están en capacidad de manejar las conexiones que las llamadas SIP generan, se requieren otros elementos que puedan hacerlo. Para esto existen soluciones como los denominados *firewall SIP-aware* con capacidades SIP o los elementos de borde SBC, como el que se usa en el producto CUBE de Cisco. El objetivo de estos elementos intermedios es aislar a la red corporativa de la red del proveedor de servicios.
- En el diseño de cualquier red, sin importar su tamaño, siempre deben ser considerados criterios de escalabilidad, seguridad, administración, calidad de servicio, entre otros. Con el análisis de estos elementos se puede alcanzar un diseño que presente las condiciones necesarias para mantener la alta disponibilidad de la red y sus servicios.
- La reingeniería de la red de datos de Alianza de Seguros para la integración de servicios de Telefonía IP, aparentemente no retorna el total de la inversión en el tiempo de vida del proyecto con los equipos cotizados, si se toma en cuenta únicamente el ahorro en el consumo telefónico como beneficio del proyecto. En este contexto se dificulta tener una recuperación

de la inversión más acelerada sin disminuir la calidad de los equipos y materiales. Sin embargo, si se tomara un periodo de tiempo mayor a los 5 años considerados, los beneficios de la Telefonía IP serían más apreciables.

- La rentabilidad de un proyecto de Telefonía IP sobresale cuando la infraestructura de red necesaria para soportar este servicio se encuentra bien implementada y tiene las características suficientes para la migración e inclusión de nuevos servicios.
- Los costos de soporte y mantenimiento para los equipos de marcas conocidas de *networking* como Cisco y HP son muy altos a pagar por año. Incluso igualan los costos de los equipos. Una alternativa es adquirir equipos con una mayor confiabilidad desde el inicio para disminuir los costos en soporte y mantenimiento.
- La documentación de red es fundamental para las futuras implementaciones de nuevos servicios y aplicaciones, así como para la evaluación y mejoramiento del rendimiento de una red.
- Los conocimientos adquiridos en las materias que componen la carrera de Redes se encuentran bien cimentadas y facilitan la adquisición de nuevos conocimientos de tecnología conforme ésta evoluciona.

5.2 RECOMENDACIONES

- La infraestructura de red propuesta para Alianza de Seguros soporta los servicios actuales más Telefonía IP. Se recomienda realizar el estudio y el diseño de la red inalámbrica de manera que se integre con el diseño del presente proyecto, para brindar movilidad a los usuarios. Se deben tomar en cuenta los teléfonos celulares inteligentes de varios miembros del

personal de la empresa para que se los incluya en el diseño de la red inalámbrica.

- En aras de mantener una excelente relación con el cliente, se recomienda que Alianza de Seguros opte por el uso de nuevas tecnologías de comunicaciones unificadas, como los son los IVR, *call center*, *software* de gestión de la relación con el cliente, etc. Estos elementos pueden ser fácilmente integrados con el sistema telefónico IP propuesto.
- Luego de la implementación de la reingeniería de la red del presente proyecto, se recomienda realizar una evaluación preliminar del rendimiento de la red con el objetivo de optimizar los parámetros de la red. De igual forma, se recomienda llevar la documentación organizada, detallada y actualizada para el desarrollo de nuevos proyectos tecnológicos que beneficien a la empresa.
- Se recomienda realizar planes de contingencia y prevención de fallas. Estos planes deben tener por objetivo disminuir el tiempo de caída de los servicios, reduciendo el tiempo de respuesta en atención y reparación de fallas.
- Una vez que los usuarios estén familiarizados con el uso de las funciones de *fax-a-email*, se recomienda eliminar las máquinas tradicionales de fax para manejar un esquema empresarial de cero papeles. Esta iniciativa permitirá a Alianza de Seguros ser reconocida por su preocupación por el medio ambiente, imprimiendo sólo los correos que sean absolutamente necesarios. En este esquema, el servidor de Telefonía IP será el encargado de enrutar los faxes entrantes a las bandejas de correo pertinentes. Una vez descargado el correo, este puede ser impreso, de requerirse, en una impresora local.

- En el caso de la migración a un sistema de cero papeles se recomienda implementar un algoritmo en el servidor de Telefonía para que los faxes puedan ser redirigidos a una impresora local disponible al momento de ser recibidos. Con ello se emula el esquema de fax tradicional a tiempo real.
- Se recomienda desarrollar un estudio para la implementación del servicio de directorio como *middleware* de la red, de manera que todos los servicios y aplicaciones basadas en MS Windows o cualquier otra plataforma pueden usar este medio para autenticación y autorización, a través de un directorio consolidado y único.
- Las políticas de seguridad planteadas en este proyecto deber ser implementadas en su totalidad, ya que se encontraron vulnerabilidades que afectan directamente a la productividad de la empresa, lo que puede ocasionar pérdidas substanciales en sus ingresos netos.
- Se recomienda la capacitación del personal técnico en el manejo de la red activa y pasiva para la evaluación de posibles daños en la infraestructura de manera que sean capaces de solventarlos de forma rápida y eficiente sin la necesidad de recurrir a los costosos servicios de consultores externos.
- Para reforzar los conocimientos adquiridos en las aulas se debería realizar proyectos con empresas que posean redes completamente funcionales para permitir un rápido involucramiento de los futuros ingenieros de la carrera en el mercado laboral.