

ESCUELA POLITÉCNICA NACIONAL

**FACULTAD DE INGENIERÍA ELÉCTRICA Y
ELECTRÓNICA**

**REINGENIERÍA DE LA INTRANET DE LA EMPRESA
TECNOMEGA C.A.**

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

AUTOR: FRANCISCO JAVIER ROMÁN SEGOVIA

Email: francisco.roman@romsegroup.com

DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO

Email: phidalgo@ieee.org

Quito, Junio 2008

DECLARACIÓN

Yo, Francisco Javier Román Segovia, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Francisco Javier Román Segovia

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Francisco Javier Román Segovia, bajo mi supervisión.

Ing. Pablo William Hidalgo Lascano
Director del Proyecto

AGRADECIMIENTOS

Tecnomega es una empresa seria que cuenta con un personal muy atento con sus clientes; este proyecto surgió con la idea de aplicar los conocimientos adquiridos durante mi carrera en un caso práctico y que mejor en una empresa con la que he tenido buenas relaciones comerciales y de amistad.

Johnny Procel el vendedor que ha atendido a mi empresa por más de 10 años, le expuse la idea y conversó con el Gerente General Ing. Johnson Silva, me recomendó y le pidió que me dé una cita para que le explicara el proyecto, le gustó la idea y me presentó al Gerente del Departamento de Sistemas el Ing. Víctor Hugo Salazar y me autorizó a que solicitara cualquier información que necesite para mi Proyecto de Titulación.

Ing. Víctor Hugo Salazar me explicó los procedimientos de la empresa y la infraestructura con la que cuenta la empresa, también me presentó al Gerente Técnico el Sr. Edwin Ávila; él me dio información más detallada de la configuración de los equipos de la red y un inventario de los equipos instalados.

Ing. Víctor Hugo Salazar también me presentó al Administrador de la Red el Ing. Guillermo Cevallos, quien me facilitó el acceso a los equipos de la red y monitoreo de los mismos. Todas estas personas y algunas que no he nombrado han brindado su atención y tiempo en la realización de este proyecto, lo cual agradezco infinitamente.

Agradezco el apoyo de mi familia y amigos que me han alentado para graduarme y ser un profesional.

DEDICATORIA

Este proyecto se lo dedico a mi familia que me ha apoyado toda mi vida y quiere lo mejor para mi, ésta es una meta para mi padres porque quieren dejar a sus hijos la mejor herencia que les pueden dar, que es una profesión.

Éste es un paso más en el que me ha apoyado mi familia desde la escuela, el colegio y hoy ya terminado la universidad, estoy consciente que éste no es el último nivel de mi educación faltan algunas maestrías y cursos, porque hay que estar permanentemente actualizado en esta profesión.

Espero siempre tener el mismo apoyo de mi familia y seguir estudiando para “ser mas para servir mejor”, el sabio refrán de mi Colegio San Gabriel. Muchas gracias a toda mi familia, mi padre, mi madre y mi hermano, les dedico este trabajo de tanto tiempo.

Francisco

CONTENIDO

1	SITUACIÓN ACTUAL DE LA INTRANET	1
1.1	INTRODUCCIÓN	1
1.2	INVENTARIO DE <i>HARDWARE</i> Y <i>SOFTWARE</i> EMPRESARIAL	6
1.2.1	<i>INVENTARIO DE EQUIPOS</i>	6
1.2.1.1	Inventario de Equipos de Computación	7
1.2.1.2	Inventario de Equipos de Conectividad LAN	7
1.2.1.2.1	Equipos de Conectividad LAN de Quito	7
1.2.1.2.2	Equipos de Conectividad LAN de Guayaquil	13
1.2.1.3	Inventario de Equipos Instalados por los Proveedores de <i>Internet</i>	15
1.2.2	<i>INVENTARIO DE SOFTWARE</i>	16
1.2.2.1	Inventario de Sistemas Operativos	16
1.2.2.2	Inventario de <i>Software</i> de Base de Datos	17
1.2.2.3	Inventario de <i>Software</i> Empresarial	19
1.2.2.3.1	Sistema Integrado Administración Corporativa	19
1.3	ENLACES ENTRE SUCURSALES Y CONEXIÓN A <i>INTERNET</i>	20
1.3.1	<i>CABLEADO ESTRUCTURADO</i>	20
1.3.2	<i>INFRAESTRUCTURA DE TELECOMUNICACIONES</i>	21
1.3.2.1	Enlaces entre las Sucursales de Quito	22
1.3.2.2	Enlaces entre las Sucursales de Guayaquil	25
1.3.3	<i>TELEFONÍA</i>	25
1.3.3.1	Sucursal Principal (Quito)	25
1.3.3.2	Sucursal Colón (Quito)	26
1.3.3.3	Sucursal CST (Quito)	27
1.3.3.4	Sucursal Sur (Quito)	28
1.3.3.5	Sucursal Mayor (Guayaquil)	29
1.3.3.6	Sucursal Sur (Guayaquil)	29
1.3.4	<i>CONEXIONES A INTERNET</i>	30
1.3.5	<i>ESPECIFICACIONES DEL HOSTING</i>	32
1.4	DIRECCIONAMIENTO <i>IP</i>	34
1.4.1	<i>DIRECCIONAMIENTO IP DE LAS SUCURSALES</i>	34
1.4.1.1	Direccionamiento <i>IP</i> de las Sucursales de Quito	34
1.4.1.2	Direccionamiento <i>IP</i> de las Sucursales de Guayaquil	35
1.4.2	<i>DIRECCIONAMIENTO IP DE LOS ENLACES ENTRE SUCURSALES</i>	36
1.4.2.1	Direccionamiento <i>IP</i> de los Enlaces entre las Sucursales de Quito	37
1.4.3	<i>DIRECCIONAMIENTO IP PARA EL SERVICIO DE INTERNET</i>	38
1.5	APLICACIONES DE LA INTRANET	39
1.5.1	<i>PERFILES DE USUARIO POR DEPARTAMENTO</i>	40
1.5.2	<i>CONSULTAS Y SERVICIOS DE LA INTRANET</i>	42

1.5.2.1	Consulta de <i>Stock</i> de Productos por Sucursal	42
1.5.2.2	Ventas por Artículo	43
1.5.2.3	Ventas por vendedor	44
1.5.2.4	Ventas Globales	44
1.5.2.5	Ventas Globales por Artículo	45
1.5.2.6	<i>Stock</i> Global	45
1.5.2.7	Depósitos Bancarios.....	46
1.5.2.8	Réplica <i>Web</i>	46
1.5.2.9	Listas de precios.....	46
1.5.2.10	Garantías.....	47
1.5.2.11	Cambiar Contraseña.....	49
1.6	SERVICIOS DEL SITIO <i>WEB</i>	50
1.6.1	REGISTRO DE USUARIOS DE LA PÁGINA <i>WEB</i>	51
1.6.2	SERVICIOS <i>WEB</i>	52
1.6.2.1	Pedido con Lista de Precios Modo Pantalla	53
1.6.2.2	Pedido con Lista de Precios Modo Impresora	53
1.6.2.3	Productos Disponibles.....	53
1.6.2.4	Lista de Precios (Formato <i>Microsoft Excel</i>)	54
1.6.2.5	Productos Llegados	54
1.6.2.6	Garantías en línea	55
1.6.2.7	Envío de Mercadería	55
1.6.3	ESQUEMA PARA CONSULTAS ENTRE SUCURSALES.....	56
1.7	ESQUEMAS DE SEGURIDAD DE LA RED	57
1.7.1	SEGURIDAD LÓGICA.....	58
1.7.1.1	Direccionamiento <i>IP</i> y Segmentación de la Red.....	59
1.7.1.2	Configuración de Equipos de Conectividad.....	60
1.7.1.3	Cambio de Claves de Acceso.....	62
1.7.1.4	Redes Privadas Virtuales (<i>VPN</i>).....	63
1.7.2	SEGURIDAD FÍSICA	63
1.7.2.1	Cuartos de Telecomunicaciones	64
1.7.2.2	Equipos de Conectividad para Seguridades de la Red.....	65
2	ANÁLISIS DE REQUERIMIENTOS Y ALTERNATIVAS TECNOLÓGICAS.....	67
2.1	ANÁLISIS DE REQUERIMIENTOS.....	67
2.1.1	REQUERIMIENTOS DE <i>HARDWARE</i>	68
2.1.1.1	Requerimientos de Equipos de Conectividad	69
2.1.2	REQUERIMIENTOS DE <i>SOFTWARE</i>	70
2.1.3	REQUERIMIENTOS DE SEGMENTACIÓN DE LA RED	72
2.1.4	ANÁLISIS DE REQUERIMIENTOS SEGURIDAD EN LA RED	73
2.2	ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS PARA EL REDISEÑO DE LA RED	74
2.2.1	TECNOLOGÍAS PARA REDES LAN.....	74

2.2.1.1	<i>Fast Ethernet</i> /	74
2.2.1.2	<i>Gigabit Ethernet</i>	76
2.2.2	TECNOLOGÍAS PARA REDES WAN Y REDES DE ACCESO	78
2.2.2.1	Línea Digital Asimétrica de Suscriptor (<i>ADSL</i>)	78
2.2.2.2	<i>Metro Ethernet</i>	80
2.2.2.2.1	Conexiones Virtuales <i>Metro Ethernet</i>	82
2.2.2.2.2	Clases de Servicio en <i>Metro Ethernet</i>	83
2.2.2.2.3	Soporte de Etiquetas para <i>VLANs</i>	83
2.2.2.2.4	Aplicaciones de <i>Metro Ethernet</i>	83
2.2.2.3	Modo de Transferencia Asíncrona (<i>ATM</i>)	84
2.2.2.3.1	Circuitos Virtuales en <i>ATM</i>	85
2.2.2.3.2	Modelo de Referencia <i>ATM</i>	86
2.2.2.4	<i>IP MPLS</i>	87
2.2.2.4.1	Arquitectura <i>MPLS</i>	88
2.2.2.4.2	Cabecera <i>MPLS</i>	89
2.2.2.5	<i>WIMAX</i>	89
2.2.2.5.1	Características de <i>WIMAX</i>	90
2.2.2.5.2	Modelos de <i>WIMAX</i>	90
2.2.2.5.3	<i>WIMAX</i> en Ecuador	92
2.2.3	TECNOLOGÍAS PARA REDES WLAN	93
2.2.3.1	Estándar <i>IEEE 802.11</i>	94
2.2.3.2	Redes Inalámbricas de Área Local <i>IEEE 802.11a</i>	95
2.2.3.3	Redes Inalámbricas de Área Local <i>IEEE 802.11b</i>	96
2.2.3.4	Redes Inalámbricas de Área Local <i>IEEE 802.11g</i>	98
2.2.3.5	Cuadro Comparativo Tecnologías de Redes Inalámbricas	100
2.2.4	TECNOLOGÍAS PARA SISTEMAS DE TELEFONÍA IP	100
2.2.4.1	Funcionalidades Telefonía <i>IP</i>	101
2.2.4.2	Movilidad	102
2.2.4.3	Ventajas de la Telefonía <i>IP</i>	102
2.2.4.4	Arquitectura Telefonía <i>IP</i>	103
2.2.4.5	Protocolos de Telefonía <i>IP</i>	103
2.2.4.6	<i>Codecs</i> para Compresión de Voz Digitalizada	104
2.2.4.6.1	Puntuación Media de Opinión (<i>MOS</i>)	105
2.2.5	TECNOLOGÍAS PARA VIDEOCONFERENCIA EN REDES IP	106
2.2.5.1	<i>Codecs</i> para Video	107
2.2.5.1.1	<i>H.263</i>	107
2.2.5.1.2	<i>H.264</i>	108
2.2.5.2	Videoconferencia una aplicación en tiempo real	108
2.2.5.3	Capacidad Videoconferencia <i>IP</i>	109
2.3	ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS PARA SEGURIDAD EN REDES	110
2.3.1	<i>Red Privada Virtual (VPN)</i>	110

2.3.1.1	Ventajas de <i>VPNs</i>	111
2.3.1.2	Requerimientos para Implementar <i>VPNs</i>	111
2.3.1.3	Tipos de <i>VPNs</i>	112
2.3.1.4	Implementaciones de <i>VPNs</i>	112
2.3.1.5	Tecnologías para <i>VPNs</i>	113
2.3.1.6	<i>IPSec</i>	114
2.3.1.6.1	Modos de Operación de <i>IPSec</i>	114
2.3.1.6.2	Protocolos de seguridad de <i>IPSec</i>	114
2.3.2	FIREWALL	115
2.3.2.1	Ventajas de los <i>Firewalls</i>	116
2.3.2.2	Desventajas de los <i>Firewalls</i>	116
2.3.2.3	Clasificación de los <i>Firewalls</i>	117
2.3.3	SISTEMA DE ANTIVIRUS DE CORPORATIVO	117
2.3.4	SISTEMA DE DETECCIÓN DE INTRUSOS	119
2.3.4.1	Tipos de <i>IDS</i>	119
2.3.5	SISTEMA DE PREVENCIÓN DE INTRUSOS	120
2.3.5.1	Tipos de <i>IPS</i>	120
2.3.6	WI-FI PROTECTED ACCESS 2 (WPA2)	121
2.3.6.1	Arquitectura 802.11i	121
2.3.7	AUTENTICACIÓN 802.1X	122
2.4	ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS DE ADMINISTRACIÓN DE RED	122
2.4.1	ELEMENTOS DEL SISTEMA DE ADMINISTRACIÓN DE RED	123
2.4.2	TIPOS DE SISTEMAS DE ADMINISTRACIÓN DE RED	124
2.4.3	ALTERNATIVAS PARA LA ADMINISTRACIÓN DE RED	125
3	ESTUDIO DE REINGENIERÍA DE LA INTRANET	127
3.1	POLÍTICAS DE SEGURIDAD	127
3.1.1	DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA RED	128
3.1.1.1	Activos a Proteger	128
3.1.1.2	Vulnerabilidades	128
3.1.1.3	Posibles Amenazas	128
3.1.1.4	Riesgos	129
3.1.1.5	Desarrollo de las Políticas de Seguridad	129
3.2	REDISEÑO DE LA RED LAN CABLEADA E INALÁMBRICA	136
3.2.1	REDISEÑO RED CABLEADA	137
3.2.1.1	Sucursales Quito	138
3.2.1.1.1	Sucursal Principal	138
3.2.1.1.2	Sucursal Colón	140
3.2.1.1.3	Sucursal CST	142
3.2.1.1.4	Sucursal Sur	144

3.2.1.2	Sucursales Guayaquil	145
3.2.1.2.1	Sucursal Mayor	145
3.2.1.2.2	Sucursal Sur	146
3.2.2	<i>RED INALÁMBRICA</i>	148
3.2.2.1	Sucursales de Quito	151
3.2.2.1.1	Sucursal Principal.....	151
3.2.2.1.2	Sucursal Colón	154
3.2.2.1.3	Sucursal CST.....	156
3.2.2.1.4	Sucursal Sur	158
3.2.2.2	Sucursales de Guayaquil	160
3.2.2.2.1	Sucursal Mayor	160
3.2.2.2.2	Sucursal Sur	163
3.3	SEGMENTACIÓN DE LA RED POR MEDIO DE <i>VLANs</i>	165
3.3.1	<i>SUCURSALES DE QUITO</i>	167
3.3.1.1	Sucursal Principal	167
3.3.1.1.1	Diseño con subredes.....	167
3.3.1.1.2	Diseño con VLSM	168
3.3.1.2	Sucursal Colón.....	169
3.3.1.2.1	Diseño por Subredes.....	169
3.3.1.2.2	Diseño por VLSM.....	170
3.3.1.3	Sucursal CST	171
3.3.1.3.1	Diseño por Subredes.....	171
3.3.1.3.2	Diseño por VLSM.....	172
3.3.1.4	Sucursal Sur.....	173
3.3.1.4.1	Diseño por Subredes.....	173
3.3.1.4.2	Diseño por VLSM.....	174
3.3.2	<i>SUCURSALES DE GUAYAQUIL</i>	174
3.3.2.1	Sucursal Mayor	175
3.3.2.1.1	Diseño por Subredes.....	175
3.3.2.1.2	Diseño por VLSM.....	176
3.3.2.2	Sucursal Sur.....	177
3.3.2.2.1	Diseño por Subredes.....	177
3.3.2.2.2	Diseño por VLSM.....	178
3.4	TELEFONÍA <i>IP</i> INTEGRADA ENTRE SUCURSALES	179
3.4.1	<i>EQUIPOS NECESARIOS PARA TELEFONÍA IP</i>	183
3.4.1.1	Centrales Telefónicas	183
3.4.1.2	Teléfonos <i>IP</i>	184
3.4.2	<i>ENLACES PARA TELEFONÍA IP</i>	185
3.4.2.1	Enlace Sucursal Principal – CST	185
3.4.2.2	Enlace Sucursal CST – Colón.....	186
3.4.2.3	Enlace Sucursal CST – Sur (Quito)	188

3.4.2.4	Enlace Sucursal Mayor (Guayaquil) – CST (Quito).....	190
3.4.2.5	Enlace Sucursal Mayor – Sur (Guayaquil).....	191
3.4.3	<i>VIDEOCONFERENCIA IP</i>	192
3.5	CÁLCULO ENLACE INTERNET Y ENLACES ENTRE SUCURSALES	194
3.5.1	CÁLCULO CAPACIDAD DE SALIDA A INTERNET	194
3.5.1.1	Sucursales de Quito.....	195
3.5.1.1.1	Sucursal Principal.....	197
3.5.1.1.2	Sucursal Colón.....	199
3.5.1.1.3	Sucursal CST.....	200
3.5.1.1.4	Sucursal Sur.....	202
3.5.1.2	Sucursales de Guayaquil.....	203
3.5.1.2.1	Sucursal Mayor.....	204
3.5.1.2.2	Sucursal Sur.....	206
3.5.2	CÁLCULO DE ENLACES ENTRE SUCURSALES	207
3.5.2.1	Enlaces Sucursales Quito.....	208
3.5.2.1.1	Enlace Sucursal Principal – CST.....	209
3.5.2.1.2	Enlace Sucursal CST – Colón.....	211
3.5.2.1.3	Enlace Sucursal CST – Sur.....	213
3.5.2.2	Enlace Quito – Guayaquil.....	215
3.5.2.2.1	Enlace Sucursal CST (Quito) – Mayor (Guayaquil).....	215
3.5.2.3	Enlaces Guayaquil.....	217
3.5.2.3.1	Enlace Sucursal Mayor – Sur.....	217
3.6	SEGURIDAD DE LA RED	219
3.6.1	SEGURIDAD FÍSICA	219
3.6.1.1	Seguridad de Equipos.....	219
3.6.1.2	Seguridad del Respaldo de Información.....	220
3.6.2	SEGURIDAD LÓGICA	221
3.6.2.1	Autenticación de Usuarios.....	222
3.6.2.2	Seguridad Red Cableada.....	225
3.6.2.2.1	VPNs entre Sucursales.....	226
3.6.2.2.2	Bloqueo de Puertos en el Firewall.....	227
3.6.2.2.3	Manejo de Vulnerabilidades.....	229
3.6.2.3	Seguridad Red Inalámbrica.....	231
3.7	ADMINISTRACIÓN DE RED	232
4	ANÁLISIS DE COSTOS DE LA SOLUCIÓN	237
4.1	COSTOS DE LAS SOLUCIONES	237
4.1.1	EQUIPOS 3COM	237
4.1.1.1	Equipos de Conectividad.....	237
4.1.1.1.1	Switches.....	237
4.1.1.1.2	Transceiver Switches.....	245

4.1.1.1.3	Ruteadores.....	245
4.1.1.1.4	Tarjetas para Ruteadores.....	246
4.1.1.1.5	Cables para Ruteadores.....	248
4.1.1.1.6	Access Points.....	248
4.1.1.1.7	Sistema Unificado de Seguridad.....	249
4.1.1.2	Centrales Telefónicas.....	251
4.1.1.3	Gateways IP.....	252
4.1.1.4	Teléfonos IP.....	253
4.1.1.5	Software de Administración de Red.....	255
4.1.2	EQUIPOS CISCO.....	257
4.1.2.1	Equipos de Conectividad.....	257
4.1.2.1.1	Switches.....	257
4.1.2.1.2	Transceiver Switches.....	262
4.1.2.1.3	Cables para Stack.....	262
4.1.2.1.4	Ruteadores.....	263
4.1.2.1.5	Módulos Ruteadores.....	266
4.1.2.1.6	Cables para Ruteadores.....	267
4.1.2.1.7	Access Point.....	269
4.1.2.2	Sistema Unificado de Seguridad.....	270
4.1.2.3	Centrales Telefónicas.....	270
4.1.2.4	Gateway IP.....	271
4.1.2.5	Teléfonos IP.....	273
4.1.2.6	Sistema de Administración de Red.....	274
4.1.3	VIDEOCONFERENCIA IP.....	275
4.1.3.1	DLINK.....	275
4.1.4	EQUIPOS NECESARIOS PARA LAS SUCURSALES Y SUS PRECIOS.....	276
4.1.4.1	Equipos 3COM.....	277
4.1.4.1.1	Sucursal Principal (Quito).....	277
4.1.4.1.2	Sucursal Colón (Quito).....	278
4.1.4.1.3	Sucursal CST (Quito).....	279
4.1.4.1.4	Sucursal Sur (Quito).....	280
4.1.4.1.5	Sucursal Mayor (Guayaquil).....	281
4.1.4.1.6	Sucursal Sur (Guayaquil).....	282
4.1.4.2	Equipos Cisco.....	283
4.1.4.2.1	Sucursal Principal (Quito).....	283
4.1.4.2.2	Sucursal Colón (Quito).....	284
4.1.4.2.3	Sucursal CST (Quito).....	285
4.1.4.2.4	Sucursal Sur (Quito).....	286
4.1.4.2.5	Sucursal Mayor (Guayaquil).....	287
4.1.4.2.6	Sucursal Sur (Guayaquil).....	288
4.1.5	SOLUCIONES PARA INTERCONEXIÓN DE SUCURSALES.....	289

4.1.5.1	<i>Telconet</i>	289
4.1.5.1.1	Enlaces de Datos.....	289
4.1.5.2	<i>PuntoNet</i>	292
4.1.5.3	Resumen y Elección de Alternativa del Servicio.....	295
4.1.5.3.1	Enlace Nacional Sucursal CST (Quito) – Sucursal Mayor (Guayaquil)	295
4.1.5.3.2	Enlace Local Sucursales de Guayaquil.....	295
4.1.5.3.3	Servicio de Internet.....	296
4.1.5.3.4	Elección del Servicio de Internet y Enlaces entre Sucursales.....	296
4.2	ANÁLISIS COSTO / BENEFICIO	297
4.2.1	<i>COSTOS DE INVERSIÓN</i>	298
4.2.2	<i>COSTOS DE OPERACIÓN</i>	299
4.2.3	<i>ESTIMACIÓN DE BENEFICIOS</i>	300
4.2.4	<i>IMPACTO DEL PROYECTO</i>	302
4.2.5	<i>SELECCIÓN DE LA SOLUCIÓN</i>	303
5	CONCLUSIONES Y RECOMENDACIONES.....	305
5.1	CONCLUSIONES	305
5.2	RECOMENDACIONES	308
	REFERENCIAS BIBLIOGRÁFICAS	311
	ANEXOS	
	ANEXO 1: INVENTARIO DE EQUIPOS DE COMPUTACIÓN	
	ANEXO 2: INVENTARIO DE COs DE LAS SUCURSALES	
	ANEXO 3: EQUIPOS UTILIZADOS EN LA IMPLEMENTACIÓN DE LOS ENLACES PRIVADOS EXISTENTES EN QUITO	

ÍNDICE DE FIGURAS

FIGURAS CAPÍTULO 1

FIGURA 1-1: SUCURSAL PRINCIPAL (QUITO).....	1
FIGURA 1-2: SUCURSAL COLÓN (QUITO).....	1
FIGURA 1-3: SUCURSAL SUR (QUITO).....	2
FIGURA 1-4: SUCURSAL CST (QUITO)	2
FIGURA 1-5: SUCURSAL MAYOR (GUAYAQUIL).....	2
FIGURA 1-6: SUCURSAL SUR (GUAYAQUIL)	2
FIGURA 1-7: ESQUEMA DE RED SUCURSAL PRINCIPAL (QUITO)	8
FIGURA 1-8: ESQUEMA DE RED SUCURSAL COLÓN (QUITO).....	9
FIGURA 1-9: ESQUEMA DE RED SUCURSAL CST (QUITO)	10
FIGURA 1-10: ESQUEMA DE RED SUCURSAL SUR (QUITO).....	11
FIGURA 1-11: EQUIPOS DE CONECTIVIDAD INSTALADOS EN LA TORRE DEL PARQUE ITCHIMBÍA.....	12
FIGURA 1-12: EQUIPOS DE CONECTIVIDAD INSTALADOS EN LA TORRE DEL VOLCÁN PICHINCHA	13
FIGURA 1-13: ESQUEMA DE RED SUCURSAL MAYOR (GUAYAQUIL).....	14
FIGURA 1-14: ESQUEMA DE RED SUCURSAL SUR (GUAYAQUIL)	15
FIGURA 1-15: ESQUEMA DE LOS ENLACES ENTRE LAS SUCURSALES DE QUITO	22
FIGURA 1-16: EQUIPOS UTILIZADOS PARA LOS ENLACES ENTRE LAS SUCURSALES DE QUITO.....	23
FIGURA 1-17: CAPACIDAD DE SALIDA A INTERNET SUCURSALES DE TECNOMEGA	31
FIGURA 1-18: ESTADÍSTICAS DE Uso <i>HOSTING</i> WWW.TECNOMEGA.COM.....	33
FIGURA 1-19: DIRECCIONAMIENTO <i>IP</i> SUCURSALES DE QUITO	35
FIGURA 1-20: DIRECCIONAMIENTO <i>IP</i> SUCURSALES DE GUAYAQUIL	36
FIGURA 1-21: DIRECCIONAMIENTO <i>IP</i> DE LOS ENLACES DE QUITO	37
FIGURA 1-22: ESQUEMA Y DIRECCIONAMIENTO DE SALIDA A <i>INTERNET</i> EN QUITO.....	38
FIGURA 1-23: ESQUEMA Y DIRECCIONAMIENTO DE LA SALIDA A <i>INTERNET</i> EN GUAYAQUIL	39
FIGURA 1-24: PANTALLA DE ACCESO A LA INTRANET	42
FIGURA 1-25: PANTALLA DE CONSULTA DE <i>STOCK</i> EN SUCURSALES.....	42
FIGURA 1-26: PANTALLA DE RESULTADOS A LA CONSULTA DE <i>STOCK</i> DE PRODUCTOS.....	43
FIGURA 1-27: PANTALLA DE VENTAS POR ARTÍCULO.....	43
FIGURA 1-28: PANTALLA DE VENTAS POR VENDEDOR.....	44
FIGURA 1-29: PANTALLA DE VENTAS GLOBALES	44
FIGURA 1-30: PANTALLA DE VENTAS GLOBALES POR ARTÍCULO.....	45
FIGURA 1-31: PANTALLA DE <i>STOCK</i> GLOBAL	45
FIGURA 1-32: PANTALLA LISTAS DE PRECIOS DE LA <i>INTRANET</i>	46
FIGURA 1-33: PANTALLA DE DESCARGAR EL ARCHIVO DE LISTA DE PRECIOS EN <i>EXCEL</i>	47
FIGURA 1-34: PANTALLA INGRESO DE GARANTÍAS (<i>RMA</i>).....	48
FIGURA 1-35: PANTALLA INGRESO DE GARANTÍAS (<i>RMA</i>) 2.....	48

FIGURA 1-36: PANTALLA PARA CAMBIO DE CLAVES DE USUARIOS	49
FIGURA 1-37: PÁGINA INICIAL WWW.TECNOMEGA.COM.....	51
FIGURA 1-38: PÁGINA DE <i>LOGIN</i> DEL USUARIO DE UNA SUCURSAL	52
FIGURA 1-39: SERVICIOS DE LA PÁGINA <i>WEB</i>	53
FIGURA 1-40: PÁGINA DE PRODUCTOS DISPONIBLES POR MARCAS O LÍNEAS	54
FIGURA 1-41: PÁGINA DE CONSULTAS DE GARANTÍAS	55
FIGURA 1-42: PÁGINA DE CONSULTA DE ENVÍO DE MERCADERÍA.....	55
FIGURA 1-43: ESQUEMA FÍSICO PARA CONSULTA DE <i>STOCK</i> EN LAS SUCURSALES.....	57
FIGURA 1-44: PANTALLA DE CONFIGURACIÓN RUTEADOR INALÁMBRICO POR DEFECTO	60

FIGURAS CAPÍTULO 2

FIGURA 2-1: ARQUITECTURA <i>METRO ETHERNET</i>	81
FIGURA 2-2: CONEXIONES VIRTUALES <i>METRO ETHERNET</i>	82
FIGURA 2-3: CABECERA <i>MPLS</i>	89
FIGURA 2-4: ESCALABILIDAD 802.11A.....	95
FIGURA 2-5: CAPACIDAD DE TRANSMISIÓN Vs. DISTANCIA 802.11A	96
FIGURA 2-6: CAPACIDAD Vs. DISTANCIA 802.11B	97
FIGURA 2-7: ESCALABILIDAD 802.11B.....	98
FIGURA 2-8: CAPACIDAD Vs. DISTANCIA 802.11G	99
FIGURA 2-9: ESCALABILIDAD 802.11G	99
FIGURA 2-10: LATENCIA Y <i>JITTER</i> EN VIDEOCONFERENCIA	109
FIGURA 2-11: ESQUEMA DE IMPLEMENTACIÓN DE UN <i>FIREWALL</i>	116
FIGURA 2-12: <i>NMS</i> SIMPLE.....	124
FIGURA 2-13: <i>NMS</i> DISTRIBUIDO.....	125

FIGURAS CAPÍTULO 3

FIGURA 3-1: ESQUEMA DE RED DE LA SUCURSAL PRINCIPAL CON CENTRAL TELEFÓNICA <i>IP</i>	139
FIGURA 3-2: ESQUEMA DE RED DE LA SUCURSAL PRINCIPAL CENTRAL TELEFÓNICA <i>IP CISCO</i>	140
FIGURA 3-3: ESQUEMA DE RED DEL REDISEÑO DE LA SUCURSAL COLÓN.....	141
FIGURA 3-4: ESQUEMA DE RED REDISEÑADA PARA LA SUCURSAL CST	143
FIGURA 3-5: ESQUEMA DE RED REDISEÑADA SUCURSAL SUR DE QUITO	145
FIGURA 3-6: ESQUEMA DE RED REDISEÑADA PARA LA SUCURSAL MAYOR DE GUAYAQUIL	146
FIGURA 3-7: ESQUEMA DE RED REDISEÑADA PARA LA SUCURSAL SUR DE GUAYAQUIL.....	147

FIGURA 3-8: ESQUEMA DE RED INALÁMBRICA.....	148
FIGURA 3-9: PLANO DEL PRIMER PISO DE LA SUCURSAL PRINCIPAL	152
FIGURA 3-10: PLANO DEL SEGUNDO PISO DE LA SUCURSAL PRINCIPAL.....	152
FIGURA 3-11: PLANO DEL PRIMER PISO DE LA SUCURSAL COLÓN	154
FIGURA 3-12: PLANO DEL SEGUNDO PISO DE LA SUCURSAL COLÓN.....	155
FIGURA 3-13: PLANO DEL PRIMER PISO DE LA SUCURSAL CST.....	157
FIGURA 3-14: PLANO DEL SEGUNDO PISO DE LA SUCURSAL CST	157
FIGURA 3-15: PLANO DEL PRIMER PISO DE LA SUCURSAL SUR DE QUITO	159
FIGURA 3-16: PLANO DEL SEGUNDO PISO DE LA SUCURSAL SUR DE QUITO.....	159
FIGURA 3-17: PLANO DEL PRIMER PISO DE LA SUCURSAL MAYOR DE GUAYAQUIL.....	161
FIGURA 3-18: PLANO DEL SEGUNDO PISO DE LA SUCURSAL MAYOR DE GUAYAQUIL	162
FIGURA 3-19: PLANO DE LA SUCURSAL SUR DE GUAYAQUIL.....	163
FIGURA 3-20: DIRECCIONAMIENTO <i>IP</i> SUCURSAL PRINCIPAL.....	168
FIGURA 3-21: DIRECCIONAMIENTO <i>IP</i> SUCURSAL COLÓN.....	170
FIGURA 3-22: DIRECCIONAMIENTO <i>IP</i> SUCURSAL CST	172
FIGURA 3-23: DIRECCIONAMIENTO <i>IP</i> SUCURSAL SUR DE QUITO.....	174
FIGURA 3-24: DIRECCIONAMIENTO <i>IP</i> SUCURSAL MAYOR	176
FIGURA 3-25: DIRECCIONAMIENTO <i>IP</i> SUCURSAL SUR DE GUAYAQUIL.....	178
FIGURA 3-26: ENLACE SUCURSAL PRINCIPAL - CST	185
FIGURA 3-27: ENLACE SUCURSAL CST- COLÓN.....	187
FIGURA 3-28: ENLACE SUCURSAL CST - SUR	189
FIGURA 3-29: ESQUEMA CONEXIÓN A <i>INTERNET</i> DE QUITO	195
FIGURA 3-30: ESQUEMA DE CONEXIÓN A <i>INTERNET</i> EN GUAYAQUIL.....	203
FIGURA 3-31: ESQUEMA RED <i>WAN</i> DE TECNOMEGA	207
FIGURA 3-32: EQUIPOS DE CONECTIVIDAD ENLACES QUITO.....	209
FIGURA 3-33: CAPACIDAD DE LOS ENLACES ENTRE SUCURSALES	216
FIGURA 3-34: <i>VPNs</i> SUCURSALES	226

FIGURAS CAPÍTULO 4

FIGURA 4-1: <i>SWITCH 3COM 5500 EI 52 PUERTOS</i>	238
FIGURA 4-2: <i>SWITCH 3COM 5500 EI 28 PUERTOS</i>	239
FIGURA 4-3: <i>SWITCH 3COM 4500 EI 26 PUERTOS</i>	241
FIGURA 4-4: <i>SWITCH 3COM 5500 EI PWR 52 PUERTOS</i>	242
FIGURA 4-5: <i>SWITCH 3COM 5500 EI PWR 28 PUERTOS</i>	243
FIGURA 4-6: <i>SWITCH 3COM 4500 EI PWR 26 PUERTOS</i>	244
FIGURA 4-7: <i>TRANSCEIVER 3COM 1000 BASE T SFP</i>	245
FIGURA 4-8: RUTEADOR <i>3COM 5012</i>	246

FIGURA 4-9: TARJETA 3COM 1 PUERTO SERIAL	246
FIGURA 4-10: TARJETA 3COM 2 PUERTOS SERIALES	247
FIGURA 4-11: TARJETA 3COM 4 PUERTOS SERIALES	247
FIGURA 4-12: ACCESS POINT 3COM 7760 802.11 A/B/G PoE	249
FIGURA 4-13: SISTEMA UNIFICADO DE SEGURIDAD 3COM X5	250
FIGURA 4-14: CENTRAL TELEFÓNICA 3COM ASTERISK	252
FIGURA 4-15: GATEWAY 3COM VCX 7111 8 PUERTOS FXO	252
FIGURA 4-16 GATEWAY 3COM VCX 7111 4 PUERTOS FXO	253
FIGURA 4-17: TELÉFONO BÁSICO 3COM 3101	253
FIGURA 4-18: TELÉFONO BÁSICO CON PARLANTE 3COM 3101	254
FIGURA 4-19: TELÉFONO DE NEGOCIOS 3COM 3102.....	254
FIGURA 4-20: 3COM ACCESS MANAGER.....	256
FIGURA 4-21: SWITCH CISCO 3750 24 PUERTOS 10/100 BASE T.....	257
FIGURA 4-22: SWITCH CISCO 3750 24 PUERTOS 10/100 BASE T PoE.....	258
FIGURA 4-23: SWITCH CISCO 3750 48 PUERTOS 10/100 BASE T.....	259
FIGURA 4-24: SWITCH CISCO 3750 48 PUERTOS 10/100 BASE T PoE.....	260
FIGURA 4-25: SWITCH CISCO 3560 24 PUERTOS 100 BASE T.....	261
FIGURA 4-26: SWITCH CISCO 3560 24 PUERTOS 100 BASE T PoE.....	261
FIGURA 4-27: MÓDULO TRANSCEIVER SFP CISCO 1000 BASE T	262
FIGURA 4-28: CABLE CISCO STACKWISE 50 CM.....	262
FIGURA 4-29: RUTEADOR CISCO 2801 VOICE BUNDLE	264
FIGURA 4-30: RUTEADOR CISCO 2811 VOICE BUNDLE	265
FIGURA 4-31: RUTEADOR CISCO 2821 VOICE BUNDLE	265
FIGURA 4-32: MÓDULO CISCO 1 PUERTO SERIAL.....	266
FIGURA 4-33: MÓDULO CISCO 2 PUERTOS SERIALES	266
FIGURA 4-34: MÓDULO CISCO 4 PUERTOS SERIALES	267
FIGURA 4-35: CABLE CISCO V.35 DTE.....	267
FIGURA 4-36: CABLE CISCO V.35 DCE	268
FIGURA 4-37: CABLE CISCO V.35 DB60.....	268
FIGURA 4-38: ACCESS POINT CISCO AIRONET 1242AG	269
FIGURA 4-39: SISTEMA DE SEGURIDAD UNIFICADO CISCO ASA CON MÓDULO IPS.....	270
FIGURA 4-40: MÓDULO CISCO 4 PUERTOS FXO	271
FIGURA 4-41: MÓDULO CISCO 2 PUERTOS FXO.....	272
FIGURA 4-42: MÓDULO CISCO 2 PUERTOS FXS	272
FIGURA 4-43: MÓDULO CISCO 4 PUERTOS FXS/DID	273
FIGURA 4-44: TELÉFONO IP CISCO 7960G	273
FIGURA 4-45: TELÉFONO IP CISCO 7942.....	274
FIGURA 4-46: EQUIPO DLINK VIDEOCONFERENCIA IP DVC-1000.....	275
FIGURA 4-47: EQUIPO DLINK VIDEOCONFERENCIA IP DVC-1100	276

ÍNDICE DE TABLAS

TABLAS CAPÍTULO 1

TABLA 1-1: INVENTARIO DE EQUIPOS INFORMÁTICOS	6
TABLA 1-2: EQUIPOS DE CONECTIVIDAD SUCURSAL PRINCIPAL (QUITO)	8
TABLA 1-3: INVENTARIO DE EQUIPOS DE CONECTIVIDAD SUCURSAL COLÓN (QUITO)	9
TABLA 1-4: INVENTARIO DE EQUIPOS DE CONECTIVIDAD SUCURSAL CST (QUITO)	10
TABLA 1-5: INVENTARIO DE EQUIPOS DE CONECTIVIDAD SUCURSAL SUR (QUITO)	11
TABLA 1-6: INVENTARIO DE EQUIPOS INSTALADOS EN EL ITCHIMBÍA	12
TABLA 1-7: INVENTARIO DE EQUIPOS DE CONECTIVIDAD INSTALADOS EN EL PICHINCHA	13
TABLA 1-8: INVENTARIO DE EQUIPOS DE CONECTIVIDAD LAN SUCURSAL MAYOR (GUAYAQUIL)	14
TABLA 1-9: INVENTARIO DE EQUIPOS DE CONECTIVIDAD SUCURSAL SUR (GUAYAQUIL)	15
TABLA 1-10: INVENTARIO DE LOS EQUIPOS PARA EL SERVICIO DE INTERNET EN LAS SUCURSALES .	16
TABLA 1-11: INVENTARIO DE SISTEMAS OPERATIVOS INSTALADOS EN LOS COMPUTADORES	17
TABLA 1-12: INVENTARIO DE SOFTWARE DE BASES DE DATOS	18
TABLA 1-13: EQUIPOS CONVERTIDORES DE FIBRA ÓPTICA	23
TABLA 1-14: INVENTARIO DE EQUIPOS PARA LOS ENLACES ENTRE LAS SUCURSALES DE QUITO	24
TABLA 1-15: DIRECCIONAMIENTO IP DE LOS EQUIPOS DE LOS ENLACES DE QUITO	24
TABLA 1-16: CONFIGURACIÓN DE LOS EQUIPOS INALÁMBRICOS PARA LOS ENLACES DE QUITO	25
TABLA 1-17: INVENTARIO DE EXTENSIONES TELEFÓNICAS SUCURSAL PRINCIPAL (QUITO)	26
TABLA 1-18: INVENTARIO DE EXTENSIONES TELEFÓNICAS SUCURSAL COLÓN (QUITO)	27
TABLA 1-19: INVENTARIO DE EXTENSIONES TELEFÓNICAS SUCURSAL CST (QUITO)	27
TABLA 1-20: INVENTARIO DE EXTENSIONES TELEFÓNICAS SUCURSAL SUR (QUITO)	28
TABLA 1-21: INVENTARIO EXTENSIONES TELEFÓNICAS SUCURSAL MAYOR (GUAYAQUIL)	29
TABLA 1-22: INVENTARIO DE EXTENSIONES TELEFÓNICAS SUCURSAL SUR (GUAYAQUIL)	29
TABLA 1-23: DIRECCIONAMIENTO IP ACTUAL DE LAS SUCURSALES DE QUITO	34
TABLA 1-24: DIRECCIONAMIENTO IP SUCURSALES DE GUAYAQUIL	35
TABLA 1-25: DIRECCIONES IP PÚBLICAS PARA CADA SUCURSAL DE QUITO	38
TABLA 1-26: DIRECCIONES IP PÚBLICAS DE LAS SUCURSALES DE GUAYAQUIL	39

TABLAS CAPÍTULO 2

TABLA 2-1: ESTÁNDARES FAST ETHERNET	76
TABLA 2-2: ESTÁNDARES GIGABIT ETHERNET	77
TABLA 2-3: COMPARACIÓN ESTÁNDARES 802.11	100
TABLA 2-4: MOS DE LOS CODECS VOIP	106
TABLA 2-5: CAPACIDAD NECESARIA PARA VIDEOCONFERENCIA IP	109
TABLA 2-6: CAPAS DEL MODELO OSI Y PROTOCOLOS DE ENCRIPCIÓN	113
TABLA 2-7: MODELO WEBEM	125

TABLAS CAPÍTULO 3

TABLA 3-1: DIMENSIONAMIENTO DE <i>SWITCHES</i> PARA LA SUCURSAL PRINCIPAL	138
TABLA 3-2: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> PARA LA SUCURSAL PRINCIPAL	138
TABLA 3-3: EQUIPOS PARA REDISEÑO DE LA SUCURSAL PRINCIPAL	139
TABLA 3-4: DIMENSIONAMIENTO EN <i>SWITCHES</i> DE LA SUCURSAL COLÓN	141
TABLA 3-5: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> DE LA SUCURSAL COLÓN	141
TABLA 3-6: EQUIPOS DEL REDISEÑO DE LA SUCURSAL COLÓN	141
TABLA 3-7: DIMENSIONAMIENTO DE <i>SWITCHES</i> PARA LA SUCURSAL CST	142
TABLA 3-8: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> DE LA SUCURSAL CST	143
TABLA 3-9: EQUIPOS DE RED PARA REDISEÑO DE LA SUCURSAL CST	143
TABLA 3-10: DIMENSIONAMIENTO EN <i>SWITCHES</i> DE LA SUCURSAL SUR DE QUITO	144
TABLA 3-11: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> DE LA SUCURSAL SUR DE QUITO	144
TABLA 3-12: EQUIPOS DE RED PARA REDISEÑADA DE LA SUCURSAL SUR DE QUITO	144
TABLA 3-13: DIMENSIONAMIENTO EN <i>SWITCHES</i> PARA LA SUCURSAL MAYOR DE GUAYAQUIL	145
TABLA 3-14: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> DE LA SUCURSAL MAYOR DE GUAYAQUIL	145
TABLA 3-15: EQUIPOS DE RED REDISEÑADA PARA LA SUCURSAL MAYOR DE GUAYAQUIL	146
TABLA 3-16: DIMENSIONAMIENTO EN <i>SWITCHES</i> PARA LA SUCURSAL SUR DE GUAYAQUIL	147
TABLA 3-17: CÁLCULO DE PUERTOS EN <i>SWITCHES</i> PARA LA SUCURSAL SUR DE GUAYAQUIL	147
TABLA 3-18: EQUIPOS DE RED REDISEÑADA PARA LA SUCURSAL SUR DE GUAYAQUIL	147
TABLA 3-19: NÚMERO DE <i>ACCESS POINTS</i> POR SUCURSAL	150
TABLA 3-20: <i>SITE SURVEY</i> SUCURSAL PRINCIPAL	153
TABLA 3-21: <i>SITE SURVEY</i> SUCURSAL COLÓN	154
TABLA 3-22: <i>SITE SURVEY</i> SUCURSAL CST	158
TABLA 3-23: <i>SITE SURVEY</i> SUCURSAL SUR DE QUITO	160
TABLA 3-24: <i>SITE SURVEY</i> SUCURSAL MAYOR	162
TABLA 3-25: <i>SITE SURVEY</i> SUCURSAL SUR DE GUAYAQUIL	164
TABLA 3-26: NÚMERO DE LAS SUCURSALES PARA EL DIRECCIONAMIENTO <i>IP</i>	166
TABLA 3-27: <i>VLANs</i> SUCURSAL PRINCIPAL	168
TABLA 3-28: <i>HOST</i> POR <i>VLAN</i> SUCURSAL PRINCIPAL	168
TABLA 3-29: <i>VLANs</i> SUCURSAL COLÓN	170
TABLA 3-30: <i>HOST</i> POR <i>VLAN</i> SUCURSAL COLÓN	170
TABLA 3-31: <i>VLANs</i> SUCURSAL CST	172
TABLA 3-32: <i>HOST</i> POR <i>VLAN</i> SUCURSAL CST	172
TABLA 3-33: <i>VLANs</i> SUCURSAL SUR DE QUITO	174
TABLA 3-34: <i>HOST</i> POR <i>VLAN</i> SUCURSAL SUR DE QUITO	174
TABLA 3-35: <i>VLANs</i> SUCURSAL MAYOR	176
TABLA 3-36: <i>HOST</i> POR <i>VLAN</i> SUCURSAL MAYOR	176
TABLA 3-37: <i>VLANs</i> SUCURSAL SUR GUAYAQUIL	178

TABLA 3-38: HOST POR <i>VLAN</i> SUCURSAL SUR GUAYAQUIL.....	178
TABLA 3-39: ASIGNACIÓN DE NÚMEROS DE EXTENSIÓN PARA LLAMADAS ENTRE SUCURSALES	179
TABLA 3-40: <i>CODECS</i> PARA TELEFONÍA <i>IP</i>	180
TABLA 3-41: CÁLCULO DE LA CAPACIDAD <i>G.711</i> PARA ENLACES <i>LAN</i>	180
TABLA 3-42: CÁLCULO DE LA CAPACIDAD <i>G.711</i> PARA ENLACES <i>WAN</i>	180
TABLA 3-43: CAPACIDAD DE TRANSMISIÓN <i>G.711</i> PARA ENLACES <i>WAN</i> CON COMPRESIÓN	181
TABLA 3-44: VALORES DE CAPACIDAD <i>LAN CODECS</i> TELEFONÍA <i>IP</i>	181
TABLA 3-45: VALORES DE CAPACIDAD <i>WAN CODECS</i> TELEFONÍA <i>IP</i>	182
TABLA 3-46: <i>CODECS</i> RECOMENDADOS PARA EL DISEÑO DEL SISTEMA DE TELEFONÍA <i>IP</i>	183
TABLA 3-47: USUARIOS Y <i>COs</i> DE LAS CENTRALES TELEFÓNICAS.....	183
TABLA 3-48: NÚMERO DE TELÉFONOS POR SUCURSAL	184
TABLA 3-49: DIMENSIONAMIENTO DE CANALES TELEFONÍA <i>IP</i> SUCURSAL PRINCIPAL	185
TABLA 3-50: DIMENSIONAMIENTO CANALES TELEFONÍA <i>IP</i> SUCURSAL COLÓN	187
TABLA 3-51: DIMENSIONAMIENTO CANALES TELEFONÍA <i>IP</i> SUCURSAL SUR DE QUITO	188
TABLA 3-52: DIMENSIONAMIENTO CANALES TELEFONÍA <i>IP</i> SUCURSAL MAYOR DE GUAYAQUIL.....	190
TABLA 3-53: DIMENSIONAMIENTO CANALES TELEFONÍA <i>IP</i> SUCURSAL CST QUITO	190
TABLA 3-54: DIMENSIONAMIENTO CANALES <i>VOIP</i> SUCURSAL SUR DE GUAYAQUIL	191
TABLA 3-55: RESUMEN CANALES TELEFONÍA <i>IP</i> SUCURSALES	192
TABLA 3-56: CAPACIDAD DE TRANSMISIÓN Vs. RESOLUCIÓN Y CUADROS POR SEGUNDO	193
TABLA 3-57: CÁLCULO DE CAPACIDAD <i>INTERNET</i> QUITO	195
TABLA 3-58: CAPACIDAD <i>ATM</i> SOBRE <i>SDH</i>	196
TABLA 3-59: ACCESO A <i>INTERNET</i> SUCURSAL PRINCIPAL QUITO	197
TABLA 3-60: ACCESO A <i>INTERNET</i> SUCURSAL COLÓN QUITO	199
TABLA 3-61: ACCESO A <i>INTERNET</i> SUCURSAL CST QUITO.....	200
TABLA 3-62: ACCESO A <i>INTERNET</i> SUCURSAL SUR QUITO	202
TABLA 3-63: CÁLCULO DE LA CAPACIDAD <i>INTERNET</i> EN GUAYAQUIL	204
TABLA 3-64: ACCESO A <i>INTERNET</i> SUCURSAL MAYOR GUAYAQUIL	204
TABLA 3-65: ACCESO A <i>INTERNET</i> DE LA SUCURSAL SUR GUAYAQUIL	206
TABLA 3-66: PUERTOS A BLOQUEAR DE INICIO DE SESIÓN.....	227
TABLA 3-67: PUERTOS A BLOQUEAR EN SERVIDORES O ESTACIONES DE TRABAJO <i>LINUX</i>	227
TABLA 3-68: PUERTOS A BLOQUEAR EN SERVIDORES CON <i>WINDOWS 2000</i>	227
TABLA 3-69: PUERTOS A BLOQUEAR EN ESTACIONES DE TRABAJO CON <i>WINDOWS XP</i>	228
TABLA 3-70: PUERTOS A BLOQUEAR EN EQUIPOS QUE NO SEAN SERVIDORES <i>DNS</i>	228
TABLA 3-71: PUERTOS A BLOQUEAR EN EQUIPOS QUE NO SEAN SERVIDORES DE CORREO	228
TABLA 3-72: PUERTOS A BLOQUEAR EN EQUIPOS QUE NO SEAN SERVIDORES <i>WEB</i>	228
TABLA 3-73: PUERTOS MISCELÁNEOS PARA BLOQUEAR EN EL <i>FIREWALL</i>	229
TABLA 3-74: EQUIPOS NECESARIOS PARA LA REINGENIERÍA DE LA RED	233

TABLAS CAPÍTULO 4

TABLA 4-1: RUTEADORES <i>CISCO</i> SERIE 2800 USUARIOS TELEFONÍA <i>IP</i>	271
TABLA 4-2: EQUIPOS <i>3COM</i> SUCURSAL PRINCIPAL (QUITO).....	277
TABLA 4-3: TELÉFONOS <i>IP 3COM</i> SUCURSAL PRINCIPAL (QUITO)	277
TABLA 4-4: EQUIPOS <i>3COM</i> SUCURSAL COLÓN (QUITO).....	278
TABLA 4-5: TELÉFONOS <i>IP 3COM</i> SUCURSAL COLÓN (QUITO)	278
TABLA 4-6: EQUIPOS <i>3COM</i> SUCURSAL CST (QUITO)	279
TABLA 4-7: TELÉFONOS <i>IP 3COM</i> SUCURSAL CST (QUITO).....	279
TABLA 4-8: EQUIPOS <i>3COM</i> SUCURSAL SUR (QUITO).....	280
TABLA 4-9: TELÉFONOS <i>IP 3COM</i> SUCURSAL SUR (QUITO)	280
TABLA 4-10: EQUIPOS <i>3COM</i> SUCURSAL MAYOR (GUAYAQUIL).....	281
TABLA 4-11: TELÉFONOS <i>IP 3COM</i> SUCURSAL MAYOR (GUAYAQUIL)	281
TABLA 4-12: EQUIPOS <i>3COM</i> SUCURSAL SUR (GUAYAQUIL)	282
TABLA 4-13: TELÉFONOS <i>IP 3COM</i> SUCURSAL SUR (GUAYAQUIL).....	282
TABLA 4-14: EQUIPOS <i>CISCO</i> SUCURSAL PRINCIPAL (QUITO).....	283
TABLA 4-15: TELÉFONOS <i>IP CISCO</i> SUCURSAL PRINCIPAL (QUITO)	283
TABLA 4-16: EQUIPOS <i>CISCO</i> SUCURSAL COLÓN (QUITO)	284
TABLA 4-17: TELÉFONOS <i>IP CISCO</i> SUCURSAL COLÓN (QUITO)	284
TABLA 4-18: EQUIPOS <i>CISCO</i> SUCURSAL CST (QUITO).....	285
TABLA 4-19: TELÉFONOS <i>IP CISCO</i> SUCURSAL CST (QUITO)	285
TABLA 4-20: EQUIPOS <i>CISCO</i> SUCURSAL SUR (QUITO).....	286
TABLA 4-21: TELÉFONOS <i>IP CISCO</i> SUCURSAL SUR (QUITO)	286
TABLA 4-22: EQUIPOS <i>CISCO</i> SUCURSAL MAYOR (GUAYAQUIL)	287
TABLA 4-23: TELÉFONOS <i>IP CISCO</i> SUCURSAL MAYOR (GUAYAQUIL)	287
TABLA 4-24: EQUIPOS <i>CISCO</i> SUCURSAL SUR (GUAYAQUIL).....	288
TABLA 4-25: TELÉFONOS <i>IP CISCO</i> SUCURSAL SUR (GUAYAQUIL).....	288
TABLA 4-26: CARACTERÍSTICAS Y COSTOS DEL ENLACE NACIONAL QUITO – GUAYAQUIL	295
TABLA 4-27: CARACTERÍSTICAS Y COSTOS DEL ENLACE LOCAL SUCURSALES DE GUAYAQUIL	295
TABLA 4-28: CARACTERÍSTICAS Y COSTOS DEL SERVICIO DE <i>INTERNET</i>	296
TABLA 4-29: COSTOS DE EQUIPOS <i>3COM</i> POR SUCURSALES	298
TABLA 4-30: COSTOS DE INSTALACIÓN ENLACES DE DATOS E <i>INTERNET</i>	298
TABLA 4-31: COSTOS SOLUCIÓN 1 (EQUIPOS <i>3COM</i>).....	298
TABLA 4-32: COSTOS DE EQUIPOS <i>CISCO</i> POR SUCURSALES	299
TABLA 4-33: COSTOS SOLUCIÓN 2 (EQUIPOS <i>CISCO</i>).....	299
TABLA 4-34: COSTOS OPERATIVOS Y DE MANTENIMIENTO	300
TABLA 4-35: ESTIMACIÓN DE BENEFICIOS DEL PROYECTO	300
TABLA 4-36: ESTIMACIÓN DE BENEFICIOS.....	301
TABLA 4-37: RESULTADOS ANÁLISIS COSTO/BENEFICIO SOLUCIÓN 1	302
TABLA 4-38: RESULTADOS ANÁLISIS COSTO/BENEFICIO SOLUCIÓN 2	302
TABLA 4-39: INDICADORES DE RENTABILIDAD DE LAS SOLUCIONES.....	303

RESUMEN

En el primer capítulo se recopila información sobre equipos de computación, conectividad, *software*, centrales telefónicas y servicios contratados por la empresa Tecnomega C.A. tales como: *Internet* y *COs* (líneas troncales); esta información es la base para el rediseño de la *Intranet*. Se detalla también el direccionamiento *IP* y el esquema de conectividad de la red en cada sucursal y los enlaces entre las sucursales de Quito.

Adicionalmente se describe la aplicación que utiliza la empresa para el manejo de ventas, inventarios y contabilidad, llamado *Global Commerce*. La página *web*, plan de *hosting* y estructura para las consultas de *stock* en las bases de datos son detallados también en el primer capítulo.

En este capítulo se describe también tanto la seguridad lógica como física, las mismas que permitirán posteriormente (capítulo 3), en función de las necesidades y vulnerabilidades de la infraestructura, desarrollar las políticas de seguridad a ser implementadas en la red. Así también se incluye en la solución equipos que incrementen la seguridad de la red, tales como: *Firewalls*, *IPS*, etc.

En el segundo capítulo, se analizan las alternativas tecnológicas para el rediseño de la red *LAN*, *WLAN* y las tecnologías de redes *WAN* disponibles en los *ISP* para los enlaces entre sucursales y el servicio de *Internet*. También se analizan las alternativas para Telefonía y Videoconferencia *IP*, la implementación de seguridades en la red y los sistemas de administración.

En el tercer capítulo se realiza el rediseño de la *Intranet*. Se dimensionan los equipos de conectividad *LAN* y *WAN*; se determinan las especificaciones que deben cumplir éstos para la implementación de una red convergente, donde se ejecuten aplicaciones de voz, datos y video.

Como complemento a la red cableada se propone implementar una red inalámbrica, teniendo acceso diferenciado de clientes y empleados al

manejar control de accesos mediante múltiples *SSID*; cada uno de ellos está asociado a una *VLAN* de clientes y otra para empleados.

El diseño del sistema de telefonía y videoconferencia *IP*, entre todas las sucursales se lo realizó como paso previo al diseño de los enlaces entre sucursales, dependiendo del *códec* utilizado. El dimensionamiento de la capacidad para *Internet* se dimensiona tomando en cuenta la capacidad necesaria para telefonía y videoconferencia *IP*.

Los enlaces entre las sucursales se dimensionan según las capacidades para ejecutar aplicaciones y servicios que requiere la empresa; estas aplicaciones serán de voz, datos y video. Se asumen datos para estos cálculos que no están ajenos a las capacidades de transmisión disponibles en Ecuador.

El diseño del esquema de seguridad física sugiere la implementación de cuartos de telecomunicaciones; la seguridad lógica requiere la instalación de un equipo de seguridad unificada con funciones de: *firewall* e *IPS*, y el sistema de antivirus corporativo. Adicionalmente, se determinan las características que debe cumplir el *software* de administración de red.

En el capítulo cuatro, se detallan los equipos para la Reingeniería de la *Intranet* en marcas *3COM* y *Cisco*, cada equipo tiene su respectivo precio y se elabora un presupuesto para cada opción. Hay que tomar en cuenta que las dos opciones son equivalentes, y tienen algunas características propias de cada marca; se escoge la opción más rentable para la empresa según al análisis costo beneficio.

En el capítulo cinco se desarrollan las conclusiones y recomendaciones a las que se ha llegado luego de la culminación del proyecto. Y por último en los anexos se detallan las tablas correspondientes al: inventario de equipos de computación de todas las sucursales, inventario de *COs* instalados en cada sucursal y equipos utilizados en la implementación de los enlaces existentes entre las sucursales de Quito.

PRESENTACIÓN

Con este proyecto se busca mejorar la disponibilidad de la red de Tecnomega, proponiendo una solución con equipos más robustos que pueden ser administrados mediante un *software* de administración de red del mismo fabricante, ya que es lo más recomendable para tener un control total de los equipos.

La integración de las sucursales de la empresa a nivel nacional es muy importante para mejorar e implementar nuevos servicios en la *Intranet*, tales como: Telefonía y Videoconferencia *IP*. Actualmente solo se tiene interconectadas las sucursales de Quito, se utiliza estos enlaces solamente para la transmisión de información y la consolidación de las bases de datos.

Se desea disminuir costos de llamadas entre sucursales y a clientes, mediante un sistema de telefonía *IP*, donde las llamadas internas sean enrutadas por los enlaces entre sucursales y las llamadas internacionales se enrutarán por *Internet*. Por ejemplo, si algún empleado de Quito realiza una llamada a un cliente en Guayaquil, la llamada se enrutará por el enlace Quito – Guayaquil y saldrá por la Sucursal Mayor, disminuyendo los costos de llamadas regionales o nacionales.

La red propuesta incorpora esquemas de seguridad física y lógica que actualmente no se tienen implementados en la empresa. También se describe las Políticas de Seguridad a implementarse que están de acuerdo con sus necesidades y su realidad.

Este proyecto puede ser un referente para futuros estudios de Reingeniería de *Intranets* para empresas de un tamaño similar o menor a Tecnomega, tomando en cuenta los servicios que se pueden implementar hoy en día en una red convergente. Los equipos y servicios que se propone se ajustan a la realidad del país, ya que son marcas y especificaciones que se comercializan en Ecuador.

CAPÍTULO 1
SITUACIÓN ACTUAL DE LA
INTRANET

1 SITUACIÓN ACTUAL DE LA *INTRANET*

1.1 INTRODUCCIÓN¹

La empresa Tecnomega C.A. se dedica a la importación y comercialización de equipos de computación, partes, piezas y accesorios. El 2 de agosto de 1999, empezó sus actividades como Mayorista de Computación, representando a diferentes marcas de prestigio internacional. Hoy en día, es el Mayorista de Computación de mayores ventas en Ecuador, por la variedad de productos y la seriedad en las garantías.

Tecnomega C.A. tiene sucursales en Quito, Guayaquil y Miami, pero para fines de este estudio solo se tomará en cuenta las sucursales a nivel nacional, cuatro en Quito y dos en Guayaquil.



Figura 1-1: Sucursal Principal (Quito)

Sucursal Principal (Quito)
Dirección: Ruiz de Castilla y Cuero y Caicedo
Esquina
PBX: 2228218 / 2502209
FAX: 2540746



Figura 1-2: Sucursal Colón (Quito)

Sucursal Colón (Quito)
Dirección: Av. Colón E2-56 entre 10 de Agosto
y 9 de Octubre
PBX: 2563036 / 056 / 058 / 074 / 2223036
FAX: 2562488

¹ Fotos e información obtenida de www.tecnomega.com



Figura 1-3: Sucursal Sur (Quito)

Sucursal Sur (Quito)
 Dirección: Ave. Maldonado S9-398 entre
 Francisco Gómez y Gil Martín
 PBX: 2651977 / 2615364 / 2653056 / 2613063



Figura 1-4: Sucursal CST (Quito)

Centro de Servicio Técnico
 Dirección: Murgueon 732 y Av. América
 PBX: 2554210 / 2908202
 FAX: 2902981



Figura 1-5: Sucursal Mayor (Guayaquil)

Sucursal Mayor (Guayaquil)
 Dirección: Calle CH entre la 11ava y 7ma # 111
 Ciudadela ADACE
 PBX: 2293755
 FAX: 2293666 Ext. 201



Figura 1-6: Sucursal Sur (Guayaquil)

Sucursal Sur (Guayaquil)
 Dirección: Ciudadela Los Almendros Manzana
 R Solar # 2 Sector Mall del Sur
 PBX: 2340479 / 2331137 / 2338475 / 2332924 /
 2349043

Tecnomega tiene más de 140 empleados en todo el país, divididos en las sucursales de Quito y Guayaquil; cuenta con alrededor de 130 computadores. En la empresa se necesita compartir dispositivos e información organizacional de las aplicaciones, entonces nació la necesidad de implementar una red de computadores que cumpla con sus expectativas.

Una red de computadores para una empresa es una poderosa herramienta de comunicaciones pudiendo tener servicios, tales como:

- Correo electrónico, para tener comunicación escrita interna y externa;
- Información consolidada en línea; disponer de los últimos cambios en la información en el menor tiempo posible es muy importante;
- Videoconferencia, comunicación audiovisual tanto interna como externa de buena calidad.

Una empresa que tiene varias sucursales en diferentes ciudades de un país o en diferentes países mediante una red convergente de voz, datos y video puede tener a sus empleados comunicados en segundos; utilizando esta tecnología les permite tener una reunión, viéndose y escuchándose unos a otros (videoconferencia), disminuyendo costos y tiempo de viajes para reuniones entre diferentes ciudades o países.

Tecnomega cuenta con una infraestructura de redes y telecomunicaciones básica, que es manejada por técnicos de la empresa. La infraestructura no ha sido planificada, ni se tiene una documentación actualizada, por lo que se tuvo que recopilar y organizar toda la información presentada en este estudio.

La red de computadores de las sucursales ha ido creciendo según las necesidades de los empleados, sin planificación en cuanto a: puntos de red, direccionamiento *IP* y equipos de conectividad. La red ha tenido serios problemas de falta de puntos de red, y se han utilizado concentradores o conmutadores para solucionarlos. Esto complica su administración, e incrementa los dominios de colisión y broadcast; disminuyendo el rendimiento integral de la red, y creando “cuellos de botella” al tener una cascada de *switches* no diseñados para esto.

Los equipos de conectividad utilizan la tecnología *Fast Ethernet* capa 2 no administrables (en su mayoría). No brindan servicios de valor agregado,

como: *VLANs*, *QoS*, administración por medio *SNMP*, protocolos de manejo de rutas redundantes, etc. Estas características de los equipos serían de mucha importancia para incrementar servicios y seguridad en la red. Con equipos de conectividad más robustos se puede lograr: segmentación por medio de *VLANs*; administración de red, facilitando la detección de fallas y disminuyendo el tiempo de solución de problemas.

El esquema de direccionamiento *IP* se ha mantenido desde inicios de la actividad de la empresa, cuando se tenían pocos usuarios en la red. Por esta razón es necesario, rediseñar el esquema de direccionamiento *IP* tomando en cuenta *VLANs* para los diferentes departamentos, donde se maneja información organizacional muy importante.

Cada día se van incrementando el número de empresas que le apuestan al comercio electrónico en el Ecuador, para comercializar sus productos dentro y fuera del país. Se comercializan productos, tales como: autos, computadores, ropa, etc.; hay países donde el comercio electrónico está muy desarrollado, como: Estados Unidos, España, Alemania, entre otros.

En Ecuador, la mayoría de instituciones financieras como los bancos tienen páginas web donde se ofrecen servicios electrónicos, como: transferencias, consultas de saldos y movimientos, pago de servicios básicos, etc. Empresas de la talla de Tecnomega no pueden quedarse sin presencia en *Internet* ni dejar de explotar el comercio electrónico.

En la página *web* de Tecnomega sus clientes pueden hacer pedidos de mercadería, consultas de *stock*, seguimiento de garantías, etc. Cada vez se van incorporando más servicios electrónicos a la página *web* dada la buena acogida que han tenido; adicionalmente se pueden hacer pedidos u ocupar los servicios electrónicos 24 horas al día los 365 días del año, logrando tener disponibilidad de información aun fuera de horario de oficina.

Los servicios de *Internet* se han contratado sin un estudio previo de la capacidad de transmisión necesaria, ocasionando molestias a los empleados porque la conexión está lenta o no está disponible. Por esta razón, se debe calcular la capacidad necesaria según aplicaciones que se quieren ejecutar.

Los proveedores de *Internet* además de la capacidad del canal que ofrecen, manejan otras características, como: factor de compartición, el cual establece el número de usuarios que están compartiendo el canal que se contrata; el tiempo garantizado de servicio, que es el tiempo que garantizan el funcionamiento del canal al año; tipo de soporte, por ejemplo se tiene que elegir entre un soporte 24 x 7 u 8 x 5 dependiendo del uso que se le va a dar y/o del horario de atención de la empresa. Estos parámetros hacen que los precios de los servicios varíen sustancialmente, teniendo que analizar los requerimientos para contratar uno u otro servicio de *Internet*.

Los enlaces entre las sucursales de Quito están subutilizados, ya que al momento se utilizan para la administración remota de los servidores, equipos de conectividad, consultas de *stock* entre las sucursales y replicación de bases de datos. Pero se puede explotar los enlaces con más aplicaciones y servicios, como: Telefonía *IP*, Videoconferencia *IP*, etc.

Los esquemas de seguridad hoy en día son muy importantes para el manejo de información empresarial. Por ello se deben establecer políticas seguridad, estableciendo procedimientos para respaldar la información y esquemas de seguridad tanto física como lógica.

Tomando un ejemplo, los cuartos de telecomunicaciones deben tener control de accesos para permitir solamente accesos autorizados, por medio de: tarjetas magnéticas, lectores biométricos, etc. Dependiendo del nivel de seguridad que se quiera dar y el precio de lo que se está protegiendo se deben escoger las medidas de seguridad a implementar en la empresa.

1.2 INVENTARIO DE *HARDWARE* Y *SOFTWARE* EMPRESARIAL

1.2.1 INVENTARIO DE EQUIPOS

En la Tabla 1-1 se muestra un resumen de los equipos de cada sucursal.

Sucursal	Computador de Escritorio	Computadores Portátiles	Servidor	Servidor de Impresión	Impresora para Red
Principal (Quito)	37	2	3	0	1
Colón (Quito)	17	0	2	0	1
Sur (Quito)	11	0	1	0	1
CST (Quito)	19	6	2	0	3
Mayor (Guayaquil)	22	1	2	0	1
Sur (Guayaquil)	9	0	2	1	0
TOTAL	115	9	12	1	7

Tabla 1-1: Inventario de Equipos Informáticos

Por medio del inventario se pueden obtener algunos datos para el rediseño de la red, tales como: número de puertos de los *switches* de las sucursales, velocidad de los puertos de los *switches*, equipos de conectividad adicionales, capacidad de los enlaces, etc.

Los servidores deben estar conectados a puertos 1000 *Base T* para tener una buena velocidad de acceso y además para que la aplicación empresarial funcione correctamente, sin interrupciones. Las estaciones de trabajo se pueden conectar a puertos de menor velocidad como 100 *Base T*, que es suficiente para ejecutar las aplicaciones de oficina en red. Los servidores de impresión y las impresoras de red también necesitan puertos 100 *Base T*.

El número de portátiles da las pautas para el diseño de la red inalámbrica en las sucursales, al momento no se tiene muchas computadoras portátiles ni de escritorio con tarjeta de red inalámbrica, pero la red inalámbrica será un complemento a la red cableada facilitando adicionar estaciones de trabajo.

1.2.1.1 Inventario de Equipos de Computación

El inventario de los equipos de computación se detalla en el Anexo 1, en éste se relaciona el computador, su sistema operativo, el tipo de computador si es de escritorio o portátil, su dirección *IP* y el departamento de la empresa al que pertenece.

1.2.1.2 Inventario de Equipos de Conectividad LAN

Los equipos de conectividad con los que se cuenta la empresa en sus diferentes sucursales, son: concentradores, conmutadores, ruteadores, ruteadores inalámbricos, servidores de impresión, etc. Los equipos son de diferentes marcas, tales como: *CNET*, *ADVANTEK*, *3COM*, *GENIUS*, entre otros. Con estos datos se puede observar la falta de planificación de la red.

A continuación se describen los equipos de conectividad instalados en cada una de las sucursales y los equipos utilizados para los enlaces entre sucursales.

1.2.1.2.1 Equipos de Conectividad LAN de Quito

Equipos de Conectividad LAN Sucursal Principal (Quito)

Los equipos de conectividad *LAN* de la Sucursal Principal, son *switches* no administrables capa 2 que sólo conmutan el flujo de datos de los computadores que conforman la red, un *hub* que conecta a dos servidores ubicados en el Departamento de Sistemas y un ruteador de banda ancha para administrar los usuarios que acceden a *Internet*. Adicionalmente, se tiene instalado un convertidor de fibra para el enlace con la Sucursal del CST.

En la Figura 1-7 se muestra el esquema de la red de esta sucursal, y en la Tabla 1-2 se detallan las características de los equipos de conectividad.

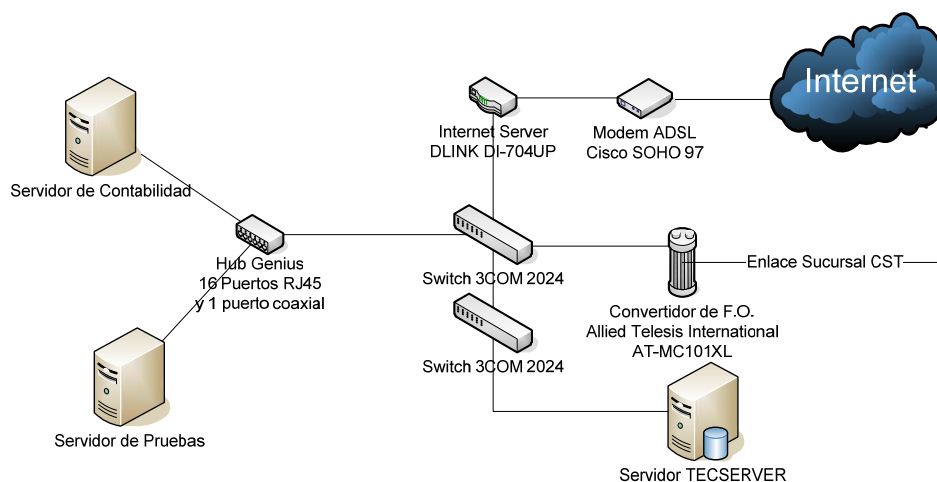


Figura 1-7: Esquema de red Sucursal Principal (Quito)

#	Marca	Modelo	Características	Tipo
1	DLINK	DI-704UP	1 puerto WAN 10/100 Base T, 4 puertos 10/100 Base T	Ruteador de Banda Ancha
2	3COM	Baseline 2024	24 puertos 10/100 Base T	Switch Capa 2 no administrable
3	3COM	Baseline 2024	24 puertos 10/100 Base T	Switch Capa 2 no administrable
4	Genius	N.D.	16 puertos 10 Base T y 1 puerto coaxial 10 Base 2	Hub
5	Allied Telesis	AT-MC101XL	1 puerto 100 Base FX y 1 puerto 100 Base TX	Convertidor de Fibra Óptica 100 Base FX a 100 Base TX

Tabla 1-2: Equipos de Conectividad Sucursal Principal (Quito)

En esta sucursal se tienen 39 usuarios que acceden a la red de forma cableada; existe falta de puntos de red en algunos departamentos por lo que se han instalado concentradores o conmutadores para solventar el problema, como es el caso del *Hub Genius* que conecta dos servidores a la red.

Equipos de Conectividad LAN Sucursal Colón (Quito)

En la Sucursal Colón se tienen dos *switches* capa 2 no administrables para la conexión de los equipos a la red; un *access point* para el enlace con la Sucursal CST con su respectiva antena parabólica. En la Tabla 1-3 se describen las principales características de los equipos mencionados.

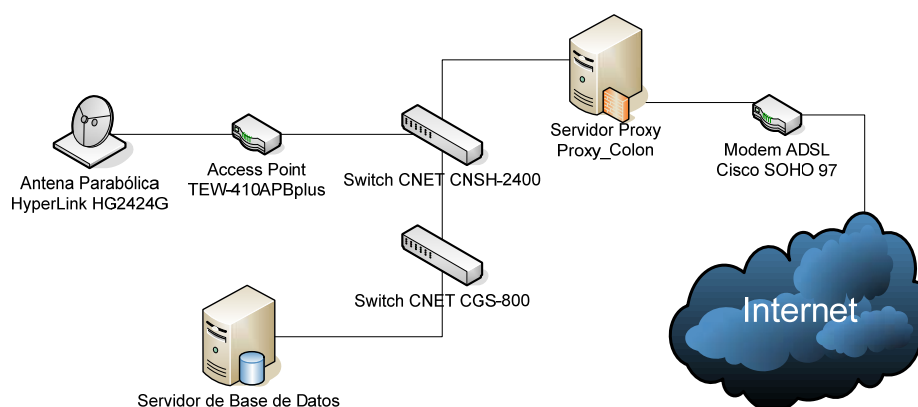


Figura 1-8: Esquema de Red Sucursal Colón (Quito)

#	Marca	Modelo	Características	Tipo
1	TRENDNet	TEW-410APBplus	1 puerto LAN 10/100 Base T	Access Point 802.11g 54 Mbps
2	HiperLink	HG2424G	Conector tipo N	Antena Parabólica 2.4 GHz, 24 dBi
3	CNET	CGS-800	8 puertos 10/100/1000 Base T	Switch Capa 2 no administrable
4	CNET	CNSH-2400	24 puertos 10/100 Base T	Switch Capa 2 no administrable

Tabla 1-3: Inventario de Equipos de Conectividad Sucursal Colón (Quito)

Equipos de Conectividad LAN Sucursal CST (Quito)

Los equipos de conectividad LAN en la Sucursal CST están distribuidos en algunos lugares del edificio. En la primera planta se tienen dos *switches*, el primero de 16 puertos para conectar los computadores y el segundo para conectar la fibra óptica del enlace con la Sucursal Principal. Los *switches* de la segunda planta son dos: uno de 16 puertos para los computadores y otro de 8 puertos para el área de servidores y el *Web Master*.

En esta sucursal se tienen los equipos para la interconexión de sucursales, éstos son: dos *access points* con sus respectivas antenas, una para el enlace con la Sucursal Colón y la otra para el enlace con la Sucursal Sur.

En la Figura 1-9 se muestra el esquema de la red de esta sucursal y en la Tabla 1-4 se detallan las características de los equipos.

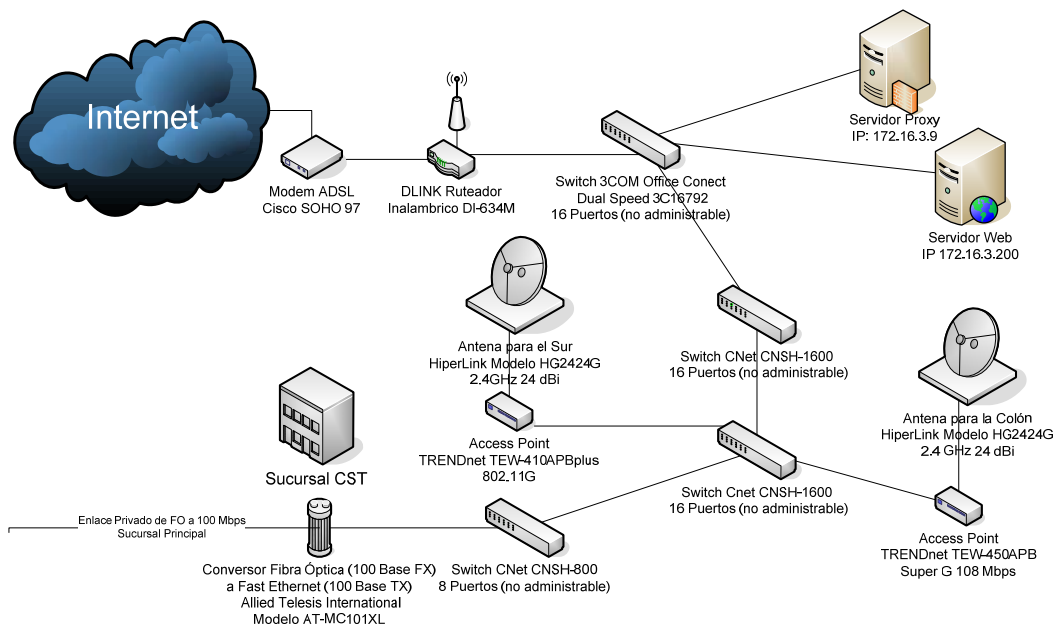


Figura 1-9: Esquema de Red Sucursal CST (Quito)

#	Marca	Modelo	Características	Tipo
1	CNET	CNSH-800	8 puertos 10/100 Base T	Switch Capa 2 no administrable
2	Allied Telesis International	AT-MC101XL	1 puerto 100 Base FX y 1 puerto 100 Base TX	Convertor de Fibra Óptica 100 Base FX a 100 Base TX
3	TRENDNet	TEW-450APB	1 puerto 10/100 Base T	Access Point Super G 108 Mbps
4	HiperLink	HG2424G	Parabólica conector N	Frecuencia 2.4 GHz 24 dBi
5	DLINK	DI-634M	1 puerto WAN RJ45, 4 puerto LAN 10/100 Base T	Ruteador Inalámbrico Banda Ancha
6	3COM	Office Connect 3C16792	16 puertos 10/100 Base T	Switch Capa 2 no administrable
7	HiperLink	HG2424G	Parabólica conector N	Frecuencia 2.4 GHz 24 dBi
8	TRENDNet	TEW-410APBplus	1 puerto 10/100 Base T	Access Point 54 Mbps
9	CNET	CNSH-1600	16 puertos 10/100 Base T	Switch Capa 2 no administrable
10	CNET	CNSH-1600	16 puertos 10/100 Base T	Switch Capa 2 no administrable

Tabla 1-4: Inventario de Equipos de Conectividad Sucursal CST (Quito)

Equipos de Conectividad Sucursal Sur (Quito)

La Sucursal de Tecnomega del Sur de Quito es nueva pero está ubicada en un edificio ya existente por lo que se adaptaron las instalaciones a sus necesidades. En esta sucursal se tienen pocos empleados (15 en total) por lo que no se tienen problemas de falta de puntos de red o instalación de *switches* en cascada para suplir la falta de puntos de red.

En la Figura 1-10, se muestra el esquema de la red en la Sucursal Sur de Quito.

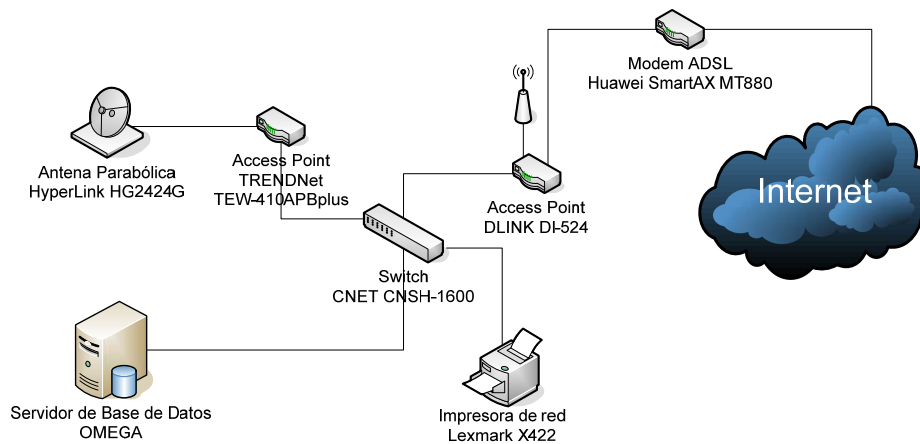


Figura 1-10: Esquema de Red Sucursal Sur (Quito)

#	Marca	Modelo	Características	Tipo
1	DLINK	DI-524	1 puerto WAN RJ45, 4 puertos LAN 10/100 Base T	Ruteador Inalámbrico de Banda Ancha 802.11g
2	TRENDNet	TEW-410APBplus	1 puerto LAN 10/100 Base T	Access Point 802.11g 54 Mbps
3	HiperLink	HG2424G	Conector tipo N	Antena Parabólica 2.4 GHz, 24 dBi
4	CNET	CNSH-1600	16 puertos 10/100 Base T	Switch (No administrable) Capa 2

Tabla 1-5: Inventario de Equipos de Conectividad Sucursal Sur (Quito)

En la Tabla 1-5 se detallan los equipos instalados: un *switch* para conectar las computadoras de los empleados, adicionalmente se tiene un *access point* y una antena para la interconexión inalámbrica con la Sucursal CST.

Equipos de Conectividad instalados en el Itchimbia

Los equipos para interconexión de las Sucursales CST y Sur están instalados en el Itchimbia, ya que se necesitaba un repetidor por la falta de línea de vista entre estas dos sucursales. Estos equipos están instalados en una torre donde se cedió a Tecnomega el derecho de uso, pero no tiene respaldo de energía por lo que si existe un apagón se cae el enlace.

Los *access points* se conectan entre sí mediante el puerto *LAN* de cada uno de ellos. En la Figura 1-11 se muestra el esquema de conexión de los equipos, y en la Tabla 1-6 se detallan las características de los mismos.

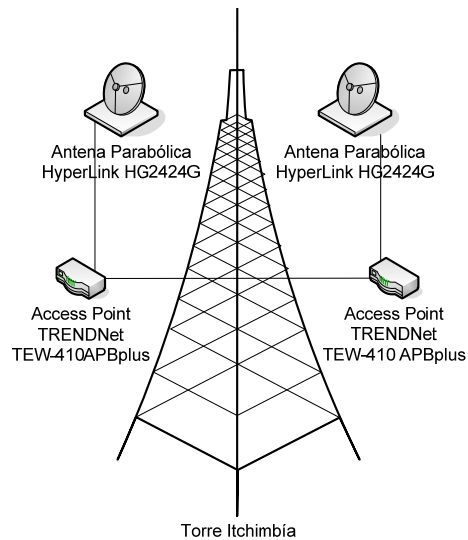


Figura 1-11: Equipos de Conectividad instalados en la Torre del Parque Itchimbia

#	Marca	Modelo	Características	Tipo
1	TRENDNet	TEW-410APBplus	1 puerto 10/100 Base T	Access Point 802.11g 54 Mbps
2	TRENDNet	TEW-410APBplus	1 puerto 10/100 Base T	Access Point 802.11g 54 Mbps
3	HiperLink	HG2424G	Parabólica, conector tipo N	Antena 2.4 GHz, 24 dBi
4	HiperLink	HG2424G	Parabólica, conector tipo N	Antena 2.4 GHz, 24 dBi

Tabla 1-6: Inventario de Equipos instalados en el Itchimbia

Equipos de Conectividad instalados en el Pichincha

Tecnomega llegó a un acuerdo para la instalación de sus antenas en una de las torres de Teleamazonas ubicada en el Volcán Pichincha; ésta tiene respaldo de energía, siendo utilizada para el enlace Sucursal CST-Colón.

Los equipos instalados en la torre del Volcán Pichincha son 2 *access points* con sus respectivas antenas, una antena apunta hacia la Sucursal CST y la segunda antena hacia la Sucursal Colón.

Los *access points* se conectan entre sí mediante el puerto *LAN* de cada uno de ellos. En la Figura 1-12 se muestra el esquema de conexión de los equipos, y en la Tabla 1-7 se detallan las características de los mismos.

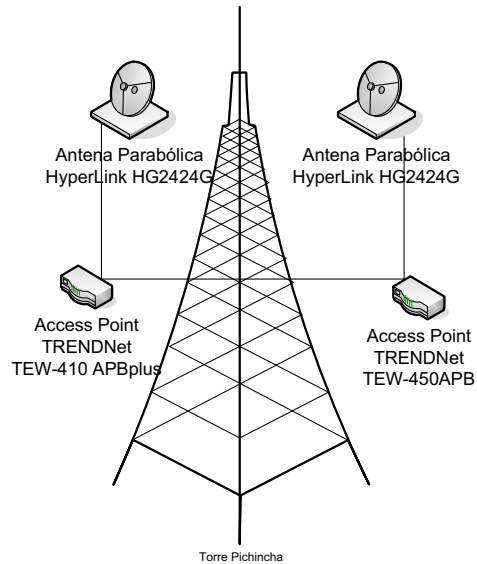


Figura 1-12: Equipos de Conectividad instalados en la Torre del Volcán Pichincha

#	Marca	Modelo	Características	Tipo
1	TRENDNet	TEW-410APBplus	1 puerto LAN 10/100 Base T	Access Point 802.11g 54 Mbps
2	TRENDNet	TEW-450APB	1 puerto LAN 10/100 Base T	Access Point Super G 108 Mbps
3	HiperLink	HG2424G	Conector Tipo N	Antena Parabólica 2.4 GHz, 24 dBi
4	HiperLink	HG2424G	Conector Tipo N	Antena Parabólica 2.4 GHz, 24 dBi

Tabla 1-7: Inventario de Equipos de Conectividad instalados en el Pichincha

1.2.1.2.2 Equipos de Conectividad LAN de Guayaquil

Equipos de Conectividad LAN Sucursal Mayor (Guayaquil)

Las sucursales de Guayaquil fueron específicamente construidas para el uso que Tecnomega requiere, por lo que no se presentan falta de puntos de red. Todos los equipos de red se han ubicado en un cuarto de telecomunicaciones.

En esta sucursal trabajan 23 personas distribuidas en varios departamentos que se conectan a la red de forma cableada. La red inalámbrica se diseñará como parte de este estudio. En la Figura 1-13 se detalla el esquema de conexión de los equipos.

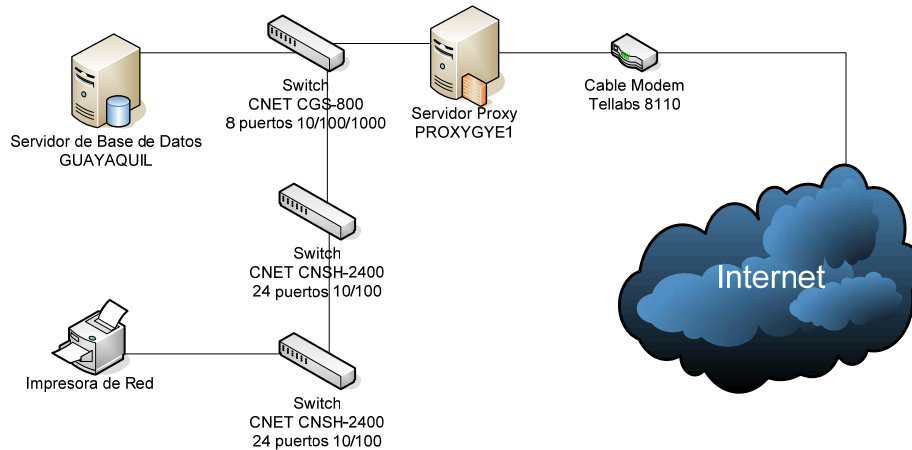


Figura 1-13: Esquema de Red Sucursal Mayor (Guayaquil)

Ésta es la sucursal más grande en Guayaquil, tiene dos *switches* de 24 puertos para los usuarios de la red y un *switch* de 8 puertos para conectar los servidores y el servicio de *Internet*. Sus especificaciones se detallan en la Tabla 1-8.

#	Marca	Modelo	Características	Tipo
1	CNET	CNSH-2400	24 puertos 10/100 Base T	Switch Capa 2 no administrable
2	CNET	CNSH-2400	24 puertos 10/100 Base T	Switch Capa 2 no administrable
3	CNET	CGS-800	8 puertos 10/100/1000 Base T	Switch Capa 2 no administrable

Tabla 1-8: Inventario de Equipos de Conectividad LAN Sucursal Mayor (Guayaquil)

Equipos de Conectividad LAN Sucursal Sur (Guayaquil)

La Sucursal Sur de Guayaquil también fue hecha a la medida de las necesidades de Tecnomega, hasta el momento no existe falta de puntos de red y se tiene un cuarto de telecomunicaciones para los equipos de conectividad. En esta sucursal trabajan 9 personas en total que se conectan a la red de forma cableada.

Los equipos de conectividad instalados son un *switch* de 24 puertos para los usuarios y un servidor de impresión para compartir impresoras que no tienen servidor de impresión incorporado, es decir no son impresoras para red.

Los equipos de conectividad *LAN* son detallados en la Tabla 1-9.

#	Marca	Modelo	Características	Tipo
1	3COM	Baseline 2024	24 puertos 10/100 Base T	Switch Capa 2 no administrable
2	DLINK	DP-300U	2 puertos paralelos y 1 puerto USB	Servidor de Impresión

Tabla 1-9: Inventario de Equipos de Conectividad Sucursal Sur (Guayaquil)

En la Figura 1-14 se muestra el diagrama de conexión de los equipos de red.

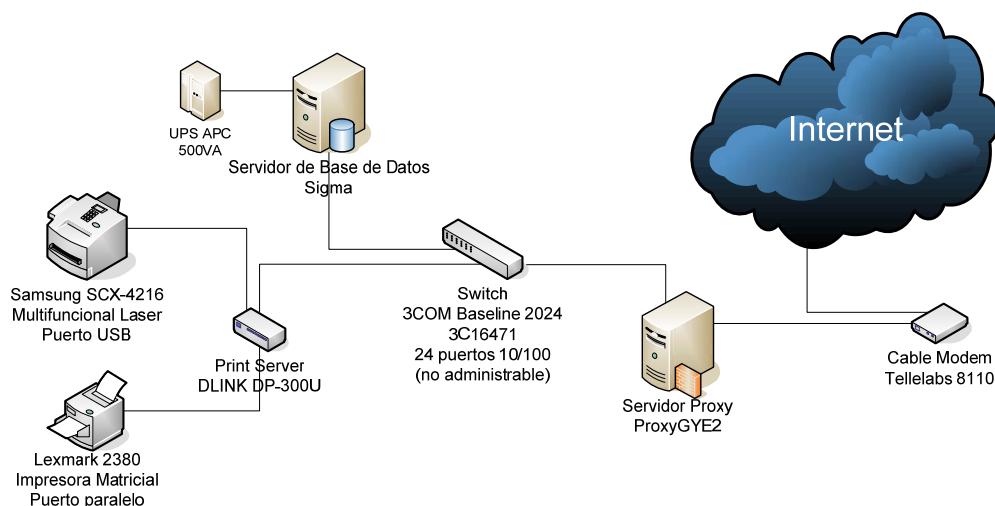


Figura 1-14: Esquema de Red Sucursal Sur (Guayaquil)

1.2.1.3 Inventario de Equipos Instalados por los Proveedores de *Internet*

Los equipos instalados por los proveedores de *Internet*, son *modems* que dependen de la tecnología del servicio que ofrecen. En Quito se contrató enlaces *ADSL* para el acceso a *Internet*, por lo tanto el proveedor instaló módems *ADSL* en una de las líneas telefónicas, para brindar este servicio.

En Guayaquil se contrató *Cable Modem* que es una tecnología que utiliza la red existente de *TVCABLE* para brindar el servicio de *Internet*, por lo que el proveedor instaló un *Cable Modem* para dar el servicio de *Internet* de Banda Ancha. En la Tabla 1-10 se detallan los equipos instalados por los dos proveedores contratados:

Sucursal	Ciudad	Equipo	Características	Proveedor
Principal	Quito	<i>Cisco SOHO 97</i>	Modem <i>ADSL</i> 1 puerto <i>WAN RJ11</i> y puerto <i>LAN 10/100 Base T</i>	Andinanet
Colón	Quito	<i>Cisco SOHO 97</i>	Modem <i>ADSL</i> 1 puerto <i>WAN RJ11</i> y puerto <i>LAN 10/100 Base T</i>	Andinanet
CST	Quito	<i>Cisco SOHO 97</i>	Modem <i>ADSL</i> 1 puerto <i>WAN RJ11</i> y puerto <i>LAN 10/100 Base T</i>	Andinanet
Sur	Quito	<i>Huawei SmartAX MT880</i>	Modem <i>ADSL</i> 1 puerto <i>WAN RJ11</i> y puerto <i>LAN 10/100 Base T</i>	Andinanet
Mayor	Guayaquil	<i>Tellabs 8110 NTU</i>	<i>Cable Modem</i> 1 puerto <i>WAN</i> y puerto <i>LAN 10/100 Base T</i>	Satnet
Sur	Guayaquil	<i>Tellabs 8110 NTU</i>	<i>Cable Modem</i> 1 puerto <i>WAN</i> y puerto <i>LAN 10/100 Base T</i>	Satnet

Tabla 1-10: Inventario de los Equipos para el Servicio de *Internet* en las Sucursales

1.2.2 INVENTARIO DE SOFTWARE

1.2.2.1 Inventario de Sistemas Operativos

La mayoría de empresas en el Ecuador utilizan *software Microsoft*, es decir Sistemas Operativos *Windows* y aplicaciones de ofimática como *Microsoft Office* y sus programas adicionales. En la Tabla 1-11 se puede notar que la plataforma de sistemas operativos de la empresa está vigente, a pesar del reciente lanzamiento del sistema operativo *Windows Vista*.

Windows XP tiene un respaldo en actualizaciones y complementos por tres años a partir del lanzamiento de *Windows Vista*; es decir, todavía *Windows XP* está vigente. Se deberá actualizar los equipos que tengan sistemas operativos caducos, tales como: *Windows 2000 Profesional*, *Windows 2000 Server* y *Windows 98 SE*.

Todos los servidores están trabajando con *Windows 2000 Server* que ya no tiene soporte. Tecnomega tiene un proyecto de migrar todos los servidores a *Windows 2003 Server*, obteniendo soporte y actualizaciones por algún tiempo más hasta tres años después que se lance *Windows 2008 Server*. Un producto de *Microsoft* pierde soporte y actualizaciones después de tres años del lanzamiento de una nueva versión del producto.

Microsoft ha anunciado que para mediados del año 2008 se lanzará al mercado *Windows Server 2008*, el cual será el próximo sistema operativo para servidores, puesto que tiene mucha más seguridad que sus antecesores y soporta más memoria *RAM*. Un sistema operativo nuevo siempre tiene problemas de compatibilidad y estabilidad, por lo que no es recomendable utilizarlos en aplicaciones críticas. Es prudente cambiar a un sistema operativo una vez que esté maduro y bien probado.

Sucursal	<i>Windows XP Pro</i>	<i>Windows 2000 Server</i>	<i>Windows 2000 Pro</i>	<i>Windows 98 SE</i>
Principal (Quito)	39	3	0	0
Colón (Quito)	16	2	0	0
CST (Quito)	23	1	3	0
Sur (Quito)	9	1	2	0
Mayor (Guayaquil)	21	1	1	2
Sur (Guayaquil)	9	1	1	0
Total	117	9	7	2

Tabla 1-11: Inventario de Sistemas Operativos Instalados en los Computadores

De la Tabla 1-11 se concluye que menos del 8% de equipos tienen sistemas operativos obsoletos, lo cual indica que el manejo de sistemas operativos cumple con las expectativas. Pero se tiene un grave problema de obsolescencia en sistemas operativos de servidores ya que se sigue utilizando *Windows 2000 Server*.

1.2.2.2 Inventario de *Software* de Base de Datos

Todos los servidores trabajan con bases de datos en *SQL Server 7.0*. Esta versión de *SQL Server 7.0* fue lanzada en 1998 y está obsoleta, sin soporte.

La siguiente versión a la que se tiene instalada es *SQL Server 2000*, que salió al mercado en el año 2000, llegó a ser la versión más utilizada.

No todas las empresas migran sus sistemas de bases de datos cada que se cambia de versión, por los altos costos de licencias. *SQL Server 2000* todavía tiene soporte hasta finales del 2008, ya que su sucesor *SQL Server 2005* salió a finales del 2005, teniendo una vigencia de tres años después del lanzamiento de una nueva versión.

Sucursal	Sistema Operativo	Sistema de Base de Datos	Nombre del Servidor
Principal (Quito)	<i>Windows 2000 Server</i>	<i>Microsoft SQL Server 7.0 SP4</i>	TECSERVER
Colón (Quito)	<i>Windows 2000 Server</i>	<i>Microsoft SQL Server 7.0 SP4</i>	BETA
Sur (Quito)	<i>Windows 2000 Server</i>	<i>Microsoft SQL Server 7.0 SP4</i>	OMEGA
Mayor (Guayaquil)	<i>Windows 2000 Server</i>	<i>Microsoft SQL Server 7.0 SP4</i>	GUAYAQUIL
Sur (Guayaquil)	<i>Windows 2000 Server</i>	<i>Microsoft SQL Server 7.0 SP4</i>	SIGMA

Tabla 1-12: Inventario de Software de Bases de Datos

Se tienen un proyecto de actualización de sistemas operativos de los servidores de *Windows 2000 Server* a *Windows 2003 Server*, donde también se actualizará los sistemas de bases de datos a *SQL Server 2000*. No se realizará una actualización a *SQL Server 2005* por costos de licencias, ya se adquirió las licencias de *SQL Server 2000*, que no se han utilizado todavía.

Para el año 2008 se lanzará *Microsoft SQL Server 2008*, con lo cual la versión de *SQL Server 2000* quedará totalmente obsoleta y sin soporte. Esto debería ser una advertencia para los encargados de la migración de las bases de datos, ya que la vigencia de un proyecto no puede ser tan corta y realizada con sistemas o programas obsoletos, en corto plazo.

Un proyecto tecnológico por lo menos debe tener una vigencia de tres años. Con este proyecto que se va a implementar no se logrará esta vigencia mínima, porque en el 2008 el *SQL Server 2000* estará totalmente obsoleto y sin respaldo. Las bases de datos son imprescindibles, por lo que no se deberá escatimar presupuesto en la actualización de este *software*.

1.2.2.3 Inventario de *Software* Empresarial

1.2.2.3.1 *Sistema Integrado Administración Corporativa*

Global Commerce fue desarrollado por *FutureSoft S.A.*, una compañía que se dedica entre otras cosas al Desarrollo del *Software* a medida, y que tiene domicilio en Guayaquil. El programa *Global Commerce* como su nombre lo dice es un Sistema Integrado para Administración Corporativa que maneja varios módulos según la necesidad de cada empresa.

Tecnomega compró algunos módulos y el código fuente para poder modificarlos y adaptarlos a sus necesidades. Estos módulos son:

- **Módulo de facturación:** dentro de las actividades de la empresa se identifican tres tipos de registros, éstos son: transacciones, consultas y reportes, mantenimiento.
- **Módulo de Inventario:** gestiona inventario de bodegas, se registran ingresos y egresos de mercadería; además cambios por garantías, casos puntuales de ingresos y egresos de mercadería.
- **Módulo de Contabilidad General:** integra todas las herramientas para la contabilidad de la empresa, incluyendo anexo transaccional.
- **Módulo de Seguridad:** el sistema tiene un esquema de seguridad que incluye claves y nombres de usuario; adicionalmente se tiene control de accesos para tipos de usuarios especificados por perfiles limitando los módulos del sistema a los que pueden acceder.
- **Módulo Cuentas por Pagar:** permite administrar todos los pagos a proveedores, órdenes de compra para proveedores, etc.
- **Módulo Cuentas por Cobrar:** permite realizar consultas de cobros pendientes en cheques, *recaps* o pagos. Además se puede obtener informes de la cartera, ventas, etc.
- **Módulo Roles de Pago:** genera el rol de pagos donde especifica el nombre del empleado, salario, los descuentos por impuestos y multas.

1.3 ENLACES ENTRE SUCURSALES Y CONEXIÓN A *INTERNET*

Las comunicaciones hoy en día son indispensables para las empresas, y más aun cuando la empresa se dedica a la rama tecnológica. Tecnomega tiene claro que *Internet* es un medio de comunicación interna y externa muy importante, por el cual puede incrementar sus ventas ampliando su mercado.

Adicionalmente la necesidad de contar con información empresarial en todas las sucursales obliga a la empresa a buscar soluciones de interconexión de sus sucursales, para implementar un sistema de información que maneje datos de volúmenes de ventas, inventarios, información de empleados, etc.

Con los enlaces entre las sucursales y la conexión a *Internet* se puede implementar una *Intranet* para manejar la información de la empresa, actualizando los datos de los servidores ubicados en cada una de las sucursales. Por eso se pensó en interconectar las sucursales y diseñar su *Intranet* para manejo de información empresarial.

Para sacar más provecho a enlaces entre sucursales y la conexión a *Internet* se diseñará un sistema de Telefonía y Videoconferencia *IP*, para disminuir costos en llamadas telefónicas regionales, nacionales o internacionales.

1.3.1 CABLEADO ESTRUCTURADO

Las sucursales antiguas de la empresa, como: la Sucursal Principal y CST de Quito; no se ha realizado cableado estructurado sino que se ha pasado cables para satisfacer las necesidades de puntos de red y se ubica un *switch* donde se necesite más puntos de red, sin cumplir ninguna norma o estándar.

En las sucursales más recientes, como: la Sucursal Colón y Sur de Quito, la Sucursal Mayor y Sur de Guayaquil se tiene instalado cableado estructurado con categoría 5E cumpliendo la norma EIA/TIA 568B, que no ha sido certificado aun.

Para manejar Fast Ethernet en instalaciones nuevas es aconsejable implementar cableado estructurado categoría 5E o superior y para Gigabit Ethernet es aconsejable cableado categoría 6 o superior.

Al no tener cableado estructurado certificado, la red puede presentar fallas y problemas relacionados con los cables, conectores, etc.; disminuyendo la disponibilidad de la red en general.

1.3.2 INFRAESTRUCTURA DE TELECOMUNICACIONES

Para la interconexión de las sucursales de Quito se tenían varios proyectos, buscando alternativas con proveedores de servicios *WAN*, pero estos servicios que se ofrecían eran muy costosos y la gerencia decidió interconectar las sucursales en forma inalámbrica, con equipos que serían adquiridos por la compañía.

Para este proyecto se comprarían los equipos y se negociarían con las empresas dueñas de torres de antenas en el Volcán Pichincha y en el parque Itchimbía para ubicar las antenas de los enlaces entre las sucursales. Estos lugares fueron determinados como estratégicos para la ubicación de las antenas, luego de realizar un estudio por una empresa contratada para esto.

Hasta el día de hoy Tecnomega no tiene un enlace de datos Quito – Guayaquil, y tampoco entre las sucursales de Guayaquil, por lo que se propondrá una tecnología específica para estos enlaces y sus capacidades; adicionalmente se analizarán las capacidades de los enlaces actuales.

1.3.2.1 Enlaces entre las Sucursales de Quito

Los enlaces entre las sucursales de Quito, se realizaron por medio de radio enlaces. Para el diseño se contrató una empresa para que realice el estudio de factibilidad y sugiera la ubicación de las antenas para su interconexión.

Se escogieron lugares donde existan torres de antenas para arrendar un espacio para las antenas de Tecnomega; se concluyó que las antenas deberían ubicarse en las torres de antenas en el Volcán Pichincha para el enlace con la sucursal Colón y el CST; y en el Parque Itchimbia para el enlace entre el CST y la sucursal Sur.

Los equipos que fueron adquiridos son *access points* TRENDNet TEW-410APBplus y TRENDNet TEW-450APB que tienen la funcionalidad de Puente Inalámbrico. Para poder cubrir la distancia requerida en los enlaces entre las sucursales, se cambiaron las antenas de los *access points* por unas de 24 dBi HiperLink modelo HG2424G, con frecuencia de 2.4 GHz.

El esquema de conexión de los equipos que integran los enlaces entre sucursales se muestra en la Figura 1 – 15.

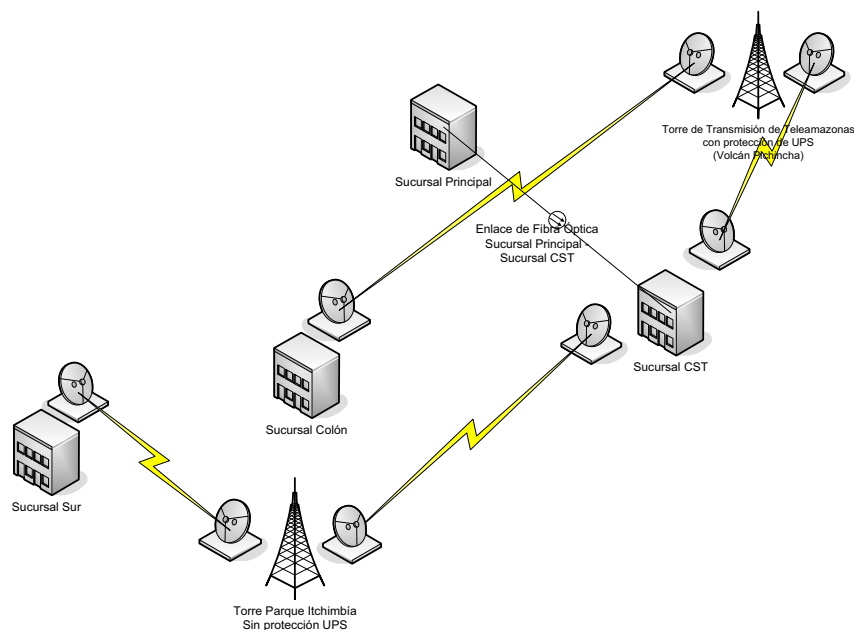


Figura 1-15: Esquema de los enlaces entre las sucursales de Quito

En la Figura 1 - 16, se observan las sucursales de la empresa y el tipo de enlaces. Se tienen enlaces inalámbricos y un enlace cableado. Los inalámbricos conectan las siguientes sucursales: Sucursal CST – Colón, Sucursal CST – Sur. El enlace cableado de fibra óptica que pasa por los postes de alumbrado público, conecta las Sucursales Principal - CST.

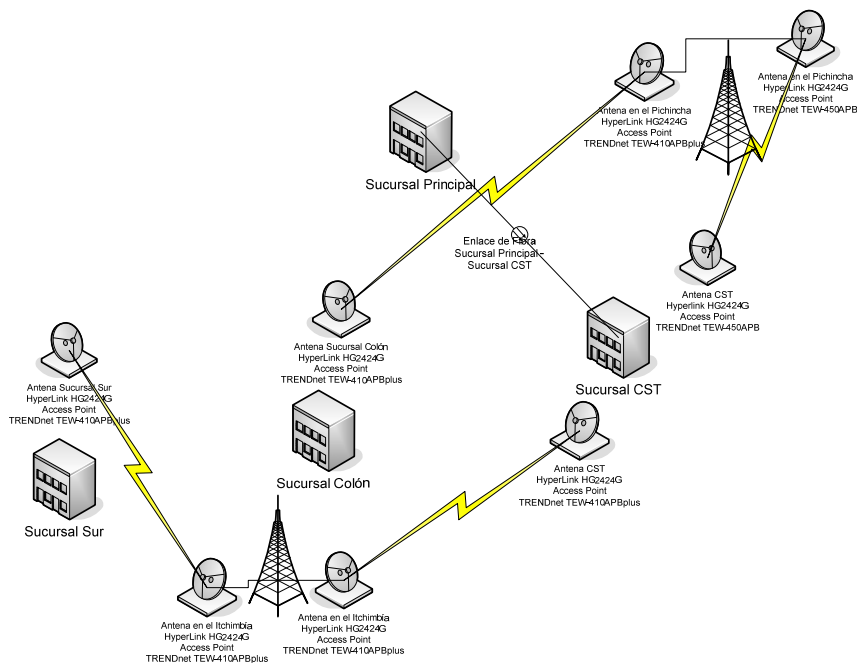


Figura 1-16: Equipos utilizados para los enlaces entre las sucursales de Quito

El enlace entre la Sucursal Principal y la Sucursal CST es de fibra óptica multimodo a 100 *Mbps*, que cumple con el estándar 100 *Base FX*. Para la conexión con la red LAN de las sucursales se deben utilizar convertidores de fibra óptica en cada uno de los extremos; estos convertidores se detallan en la Tabla 1 – 13.

Cantidad	Equipo	Modelo	Características
2	Allied Telesis Internacional	AT-MC101XL	Convertidor Fibra Óptica 100 <i>Base FX</i> a 100 <i>Base TX</i>

Tabla 1-13: Equipos Convertidores de Fibra Óptica

Estos convertidores de medios son no administrables y están trabajando en modo *full* dúplex, esto se logra con dos fibras (una para transmisión y otra para recepción). La fibra óptica que se utilizó para el enlace es una fibra óptica multimodo para una longitud máxima de 2 Km; en sus extremos se conecta a los equipos conversores por medio de conectores *ST*.

El resto de enlaces entre las sucursales de Quito son enlaces inalámbricos que trabajan a 5 Mbps, mediante *access points* TRENDNet en modo de puente inalámbrico. En la Tabla 1-14 se detallan los equipos de los enlaces.

Nombre Equipo	Equipo	Enlace	Dirección IP
Murgueon	TEW-450APB	Sucursal CST – Antena CST en el Pichincha	193.169.10.205
Pich-Murgueon	TEW-450APB	Antena CST – Antena Colón en el Pichincha	193.169.10.203
Pich-Colón	TEW-410APBplus	Antena Colón en el Pichincha - Sucursal Colón	193.169.10.195
Colón	TEW-410APBplus		193.169.10.196
Murgueon	TEW-410APBplus	Sucursal CST – Antena CST en el Itchimbía	192.168.10.25
P-Murgueon	TEW-410APBplus	Antena CST – Antena Sur en el Itchimbía	192.168.10.24
P-Sur	TEW-410APBplus	Antena Sur en el Itchimbía – Sucursal Sur	192.168.10.23
Sur	TEW-410APBplus		192.168.10.22

Tabla 1-14: Inventario de Equipos para los enlaces entre las sucursales de Quito

En la Tabla 1-15 se puede determinar qué equipo se conecta de uno y otro extremo en el enlace por medio de las direcciones MAC; para tener una mayor facilidad de determinar los equipos enlazados se detallan las direcciones IP de los equipos y su equipo remoto.

Nombre Equipo	Dir. IP Local	MAC Local	MAC Remoto	Dir. IP Remoto
Murgueon	193.169.10.205	00:03:2F:2F:24:B3	00:03:2F:2E:E9:C8	193.169.10.203
Pich-Murgueon	193.169.10.203	00:03:2F:2E:E9:C8	00:03:2F:2F:24:B3	193.169.10.205
Pich-Colón	193.169.10.195	00:0E:8E:7A:6F:12	00:0E:8E:7A:6D:0B	193.169.10.196
Colón	193.169.10.196	00:0E:8E:7A:6D:0B	00:0E:8E:7A:6F:12	193.169.10.195
Murgueon	192.168.10.25	00:0E:8E:7A:67:7B	00:0E:8E:7A:6F:23	192.168.10.24
P-Murgueon	192.168.10.24	00:0E:8E:7A:6F:23	00:0E:8E:7A:67:7B	192.168.10.25
P-Sur	192.168.10.23	00:0E:8E:7A:7B:69	00:0E:8E:7A:6E:9F	192.168.10.22
Sur	192.168.10.22	00:0E:8E:7A:6E:9F	00:0E:8E:7A:7B:69	192.168.10.23

Tabla 1-15: Direccionamiento IP de los equipos de los enlaces de Quito

La configuración de los equipos no es correcta, ya que existe solapamiento entre los canales 2 y 3 (canales contiguos), generando interferencia entre ellos. Adicionalmente, el SSID de los *access points* del enlace Sucursal Murgueon - Sur tiene el SSID por defecto, lo cual muestra que no se tiene un esquema de seguridad inalámbrica, teniendo en cuenta que los equipos no tienen ningún esquema de autenticación habilitada.

Nombre Equipo	SSID	Canal	Modo Inalámbrico	Seguridad
Murgueon	TECNOMEGA	3	11g	Deshabilitada
Pich-Murgueon	TECNOMEGA	3	11g	Deshabilitada
Pich-Colón	TECNOMEGA	11	11g	Deshabilitada
Colón	TECNOMEGA	11	11g	Deshabilitada
Murgueon	ap11g	2	11g	Deshabilitada
P-Murgueon	ap11g	2	11g	Deshabilitada
P-Sur	ap11g	3	11g	Deshabilitada
Sur	ap11g	3	11g	Deshabilitada

Tabla 1-16: Configuración de los Equipos Inalámbricos para los enlaces de Quito

La configuración de los equipos baja su eficiencia ya que están trabajando en modo *802.11b* y *802.11g*, si no se utilizan equipos *802.11b* en los enlaces se debería deshabilitar la compatibilidad con *802.11b* para tener una mejor eficiencia en los enlaces.

1.3.2.2 Enlaces entre las Sucursales de Guayaquil

Las Sucursales de Tecnomega en Guayaquil, no tienen un enlace entre ellas. Tampoco están enlazadas las Sucursales de Guayaquil con las de Quito, por lo que no se presentará información al respecto.

1.3.3 TELEFONÍA

1.3.3.1 Sucursal Principal (Quito)

En esta sucursal se tiene instalada una central telefónica Híbrida *Panasonic KX-TDA200*; al momento se tienen funcionando 20 extensiones analógicas de 24 disponibles y 13 digitales de 16 disponibles. Se tienen contratados 21 COs² analógicos con Andinatel.

² *Central Office (CO)* son las líneas telefónicas que conectan al usuario y la oficina central de la empresa de telefonía, estas líneas están conectadas a un equipo de conmutación para que puedan comunicarse las líneas entre sí localmente y a larga distancia.

Sucursal Principal (Quito)		
Departamento	# Personas	# Extensiones
Administrativo	8	8
Ventas	9	9
Bodega	5	2
Crédito	5	5
Auditoría Externa	2	1
Caja	3	1
Contabilidad	3	2
Técnico	2	1
Sistemas	2	1
Datafast	0	3
TOTAL	39	33

Tabla 1-17: Inventario de Extensiones Telefónicas Sucursal Principal (Quito)

Se puede concluir, no todos los empleados tienen una extensión telefónica propia, las razones son variadas. Algunos empleados no tienen una extensión exclusiva porque son nuevos y no existe el cableado necesario para asignarles una extensión o porque en el departamento en que trabajan tienen alta movilidad y no se les ha asignado una extensión.

La Sucursal Principal es la sucursal más grande de la empresa, ubicada en Ruiz de Castilla 820 y Cuero y Caicedo, allí trabajan alrededor de 40 personas. Por esta razón se necesita una gran cantidad de líneas telefónicas para que los clientes llamen a sus vendedores y para que los empleados se comuniquen con los clientes y con otros empleados de la empresa ubicados en otras sucursales.

El inventario de los COs de la Sucursal Principal se detalla en el Anexo 2, se muestra el número de COs y su respectivo número de telefónico.

1.3.3.2 Sucursal Colón (Quito)

En la sucursal Colón de Quito se tiene instalada una central telefónica *Panasonic TDA-100BX* Híbrida *IP-PBX*, la cual tiene funcionado 16 extensiones, 15 de ellas son digitales y 1 analógica. Adicionalmente se tienen contratados para la sucursal 15 COs con Andinatel.

Sucursal Colón (Quito)		
Departamento	# Personas	# Extensiones
Administrativo	2	2
Bodega	3	2
Caja	2	1
Crédito	2	2
Ventas	7	7
Técnico	1	1
Datafast	0	1
TOTAL	17	16

Tabla 1-18: Inventario de Extensiones Telefónicas Sucursal Colón (Quito)

La Sucursal Colón es una sucursal nueva, ubicada en Colón E2-56 entre 10 de Agosto y 9 de Octubre, donde se evidencia la planificación de instalaciones eléctricas y telefónicas. De 17 empleados, 16 tienen una extensión telefónica propia, solo en caja no se tienen dos extensiones porque no es necesario y en caso de necesitar el teléfono pueden compartir una extensión telefónica.

1.3.3.3 Sucursal CST (Quito)

En la Sucursal CST está instalada una central telefónica Híbrida Panasonic *KX - TDA100*, la cual tiene dos tarjetas adicionales para manejar hasta 24 extensiones digitales, de las cuales se utilizan 17. Los COs que maneja esta central son 14 líneas telefónicas analógicas de Andinatel, y la tarjeta instalada puede manejar hasta 16 COs analógicos.

Sucursal CST (Quito)		
Departamento	# Personas	# Extensiones
Administrativo	2	2
Caja	1	1
Garantías	2	2
Mercadeo	7	5
Sistemas	1	1
Técnico	10	6
TOTAL	23	17

Tabla 1-19: Inventario de Extensiones Telefónicas Sucursal CST (Quito)

La Sucursal CST es una casa ubicada en la calle Murgeón 732 y Av. América, adaptada a las necesidades de la empresa por lo que se puede observar que las extensiones telefónicas no están de acuerdo con las necesidades actuales de la empresa.

En esta sucursal se tienen instaladas 14 COs, ya que en ella trabajan alrededor de 10 técnicos y el personal de Mercadeo de Quito (7 personas), que demandan de mucho uso del servicio telefónico para comunicarse con los clientes.

1.3.3.4 Sucursal Sur (Quito)

La Sucursal Sur de Quito tiene instalada una central telefónica Panasonic *TDA-100BX* Híbrida *IP-PBX*, la cual está funcionando con 10 extensiones: 9 digitales para los empleados y 1 analógica para el *Datafast*. Adicionalmente se tienen 8 COs contratados con Andinatel.

Esta sucursal es una de las más pequeñas de la empresa y funciona en un edificio ubicado en el sur de Quito, en la Av. Maldonado S9-406 y Francisco Gómez. No se tienen problemas de falta de extensiones telefónicas dado que se realizaron nuevas instalaciones telefónicas en la remodelación de esta sucursal.

Los COs contratados con Andinatel son casi igual al número de empleados; se los contrató por razones de crecimiento futuro y de escasez de líneas telefónicas en el sector de la sucursal.

Sucursal Sur (Quito)		
Departamento	# Personas	# Extensiones
Administrativo	2	2
Bodega	2	1
Caja	2	1
Ventas	4	4
Técnico	1	1
Datafast	0	1
TOTAL	11	10

Tabla 1-20: Inventario de Extensiones Telefónicas Sucursal Sur (Quito)

1.3.3.5 Sucursal Mayor (Guayaquil)

En la Sucursal Mayor de Guayaquil ubicada en Calle CH entre onceava y séptima #111 Ciudadela Adace, se tiene instalada una Central Telefónica *Panasonic TDA-100BX* Híbrida *IP-PBX*, que funciona con 18 extensiones, 10 extensiones digitales y 8 analógicas; se tienen instalados 9 COs de Pacifictel.

Sucursal Mayor (Guayaquil)		
Departamento	# Personas	# Extensiones
Administrativo	3	3
Bodega	4	1
Caja	2	1
Contabilidad	1	1
Crédito	1	1
Mercadeo	2	1
Técnico	3	2
Ventas	7	7
Datafast	0	1
TOTAL	23	18

Tabla 1-21: Inventario Extensiones Telefónicas Sucursal Mayor (Guayaquil)

Esta sucursal fue recientemente construida con una planificación adecuada en cuanto a las extensiones telefónicas, pero no pasa lo mismo con los COs por la escasez que se tiene en el sector donde está ubicada la sucursal.

1.3.3.6 Sucursal Sur (Guayaquil)

La Sucursal Sur de Guayaquil, ubicada en Cdla. Los Almendros Manzana R Solar #2, tiene instalada una Central Telefónica *Panasonic TDA-100BX* Híbrida *IP-PBX*, la cual dispone de 10 extensiones: 9 extensiones digitales para los empleados y 1 extensión analógica para el *Datafast*. Adicionalmente se tienen contratados 6 COs analógicos contratados con Pacifictel.

Sucursal Sur de Guayaquil		
Departamento	# Personas	# Extensiones
Administrativo	2	2
Bodega	2	2
Caja	1	1
Ventas	3	3
Técnico	1	1
Datafast	0	1
TOTAL	9	10

Tabla 1-22: Inventario de Extensiones Telefónicas Sucursal Sur (Guayaquil)

De la Tabla 1-22 se puede concluir que la Sucursal Sur de Guayaquil es la única donde se tiene una extensión por empleado, esto se da porque es una sucursal nueva construida a la medida y planificada con un crecimiento futuro. En cuanto a los COs guardan relación al número de empleados.

1.3.4 CONEXIONES A *INTERNET*

Todas las sucursales de Tecnomega a nivel nacional están conectadas a *Internet*, cada una tiene una conexión independiente. Las sucursales de Quito tienen como proveedor del servicio de *Internet* a Andinanet, con el cual se ha contratado cuatro enlaces *ADSL*, con las siguientes características:

- Sucursal Principal, tiene un canal 512 / 256 *Kbps* compartido 8 a 1.
- Sucursal CST, posee un canal 512 / 256 *Kbps* con compartición 8 a 1.
- Sucursal Colón, posee un canal 512/ 256 *Kbps* con compartición 8 a 1.
- Sucursal Sur, posee un canal 256 / 128 *Kbps* con compartición 8 a 1.

Las sucursales de Tecnomega en Guayaquil tienen como proveedor de Internet a SURATEL; el acceso se da por medio de *CABLE MODEM*, utilizando la infraestructura de red de Fibra Óptica de *TVCABLE*. Desde el poste de alumbrado público se utiliza un convertidor de medios para que en el cliente se utilice cable coaxial. Las características de los enlaces son:

- Sucursal Mayor, posee un canal de 512 *Kbps* de *CIR* compartido 4 a 1
- Sucursal Sur, posee un canal de 256 *Kbps* de *CIR* compartido 4 a 1

Estos planes de servicio contratados son muy básicos, es decir no soportan las aplicaciones de Telefonía *IP* y Videoconferencia *IP* a ejecutarse sobre *Internet*, debiéndose especificar las características y las tecnologías sugeridas en el Rediseño de la red.

En la Figura 1-17 se detalla el tipo de conexión de cada sucursal y su capacidad.

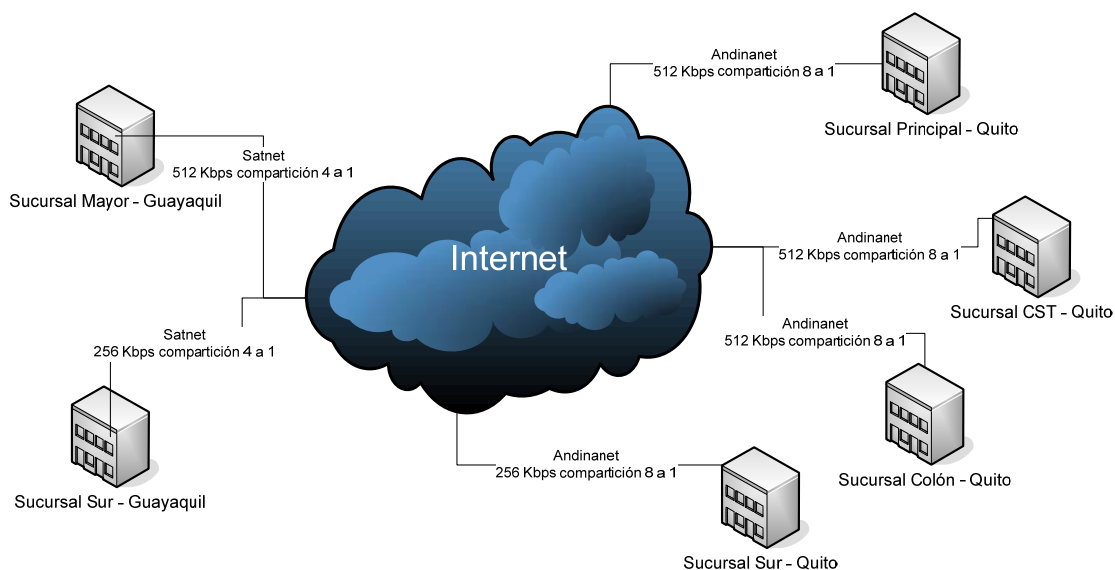


Figura 1-17: Capacidad de salida a Internet Sucursales de Tecnomega

Adicionalmente, el uso de la capacidad de *Internet* debe ser controlado y restringido para actividades que vayan acorde con el uso normal de oficina, es decir se bloquearán aplicaciones de descarga *P2P* y páginas *web* con contenidos sexuales o que distraigan a los empleados.

Existen administradores de ancho de banda en implementaciones de *software* y *hardware*, para optimizar la capacidad contratada de *Internet*. Los administradores de ancho de banda, restringen el acceso a determinados protocolos o aplicaciones que no deben ser usadas en la oficina y consumen demasiada capacidad de *Internet*, como por ejemplo: programas *P2P*, mensajería instantánea, etc. En Capítulo 4 se determinará qué tipo de implementación se utilizará.

El sistema de antivirus corporativo también ayudará con el correcto uso de la capacidad de *Internet*, ya que un computador infectado con algún tipo de *malware* puede enviar archivos a través de la red hacia *Internet* y colapsarla; peor aun si más de un equipo de la red está infectado y envían archivos para propagar el virus por *email* o un gusano que se difunde por sí solo.

1.3.5 ESPECIFICACIONES DEL *HOSTING*

El plan de *Hosting* de Tecnomega está contratado en *Yahoo*, correspondiendo al plan profesional con las siguientes especificaciones:

Plan Profesional:

- Espacio en el servidor: 20 GB
- Número de páginas soportadas: 5 a más de 100000
- Transferencia de datos mensual: 500 GB
- Número de visitantes por mes soportados: 10000 – 1.2 millones
- Direcciones de *email*: 1000
- Registro de Dominio gratis: Si
- Herramientas fáciles para crear sitios profesionales: Si
- Soporte para herramientas de diseño (*FrontPage* y *Dreamweaver*): Si
- Herramientas para *scripts* y bases de datos (*PHP*, *Perl* y *MySQL*): Si
- Soporte gratis por teléfono 24 horas: Si
- Panel de Control de uso amistoso: Si
- Mejoramientos del sitio *web* (como libros y contadores de visitas): Si
- Costo mensual: US \$ 39,95
- Costo de inscripción: US \$ 25,00

El espacio usado en el *Hosting* es de 345.50 MB de 20 GB disponibles, por lo que está subutilizada la capacidad del plan contratado. Existen planes en *Yahoo*, con capacidades menores y a menor costo, tales como:

Plan Principiante:

- Espacio en el servidor: 5 GB
- Número de páginas soportadas: 5 a más de 25000 páginas
- Transferencia de datos mensual: 200 GB
- Número de visitantes por mes soportados: 10000 – 500000
- Direcciones de *email*: 200
- Registro de Dominio gratis: Si

- Herramientas fáciles para crear sitios profesionales: Si
- Soporte para herramientas de diseño (*FrontPage* y *Dreamweaver*): Si
- Herramientas para *scripts* y bases de datos (*PHP*, *Perl* y *MySQL*): Si
- Soporte gratis por teléfono 24 horas: Si
- Panel de Control de uso amistoso: Si
- Mejoramientos del sitio *web* (como libros y contadores de visitas): Si
- Costo mensual: US \$ 11,95
- Costo de inscripción: US \$ 25,00

En la Figura 1-18 se muestran los datos estadísticos del *hosting* actual de Tecnomega.



Figura 1-18: Estadísticas de Uso *Hosting* www.tecnomega.com

El plan principiante se ajusta más a las necesidades de la empresa, ya que:

- Se tienen menos de 200 empleados, serían suficientes 200 *emails*.
- 5 GB es más que suficiente, ya que se tienen 345.5 MB usados del espacio contratado.
- La transferencia de archivos del mes de abril 2007 es la más alta registrada de 7.79 GB, siendo esta cifra menor a la ofrecida de transferencia mensual de *Yahoo* de 200 GB.

Es recomendable contratar el plan de *Hosting* Principiante para tener una mejor relación precio y porcentaje utilizado del producto contratado, ya que no se utiliza ni la mitad que el *Hosting* Principiante y se tiene contratado el *Hosting* Profesional. Por esta razón no justifica pagar por un producto que no se lo aprovecha bien.

1.4 DIRECCIONAMIENTO *IP*

El direccionamiento *IP* no se lo rediseñó al incrementar las sucursales, sino que se asignaron direcciones *IP* aleatoriamente en cada sucursal y no se tiene una política de asignación de direcciones *IP* a los equipos. Adicionalmente se deben documentar las direcciones *IP* asignadas a un computador e implementar un mecanismo para que los usuarios no puedan cambiar las mismas, con fines de ingresar a otras redes a las cuales no tienen permiso.

1.4.1 DIRECCIONAMIENTO *IP* DE LAS SUCURSALES

1.4.1.1 Direccionamiento *IP* de las Sucursales de Quito

El direccionamiento *IP* utilizado en las sucursales de Quito son direcciones clase B; este tipo de direcciones *IP* tiene 16 *bits* para la parte de *host*, por lo que se tiene en una red para 65536 computadores, con máscara de 16 *bits*. En cada Sucursal máximo se tienen 50 computadores, incluyendo los computadores de pruebas del departamento técnico. Por esta razón se debería segmentar la red en subredes para incrementar la seguridad y aumentar su rendimiento, al dividirla en varios dominios de colisión.

Sucursal	Dirección de Red	Tercer octeto que diferencia la sucursal en la red	Máscara	# de computadores
Principal	172.16.0.0	172.16.3.0	255.255.0.0	42
Colón	172.16.0.0	172.16.2.0	255.255.0.0	21
CST	172.16.0.0	172.16.5.0	255.255.0.0	32
Sur	172.16.0.0	172.16.4.0	255.255.0.0	14

Tabla 1-23: Direccionamiento *IP* Actual de las Sucursales de Quito

Se tiene una sola red para todas las sucursales de Quito, la red es clase B: 172.16.0.0 con máscara 255.255.0.0. Para diferenciar cada una de las sucursales se ha utilizado un grupo de direcciones *IP* que tienen en común el tercer octeto de la dirección de red, pero no se ha segmentado en subredes.

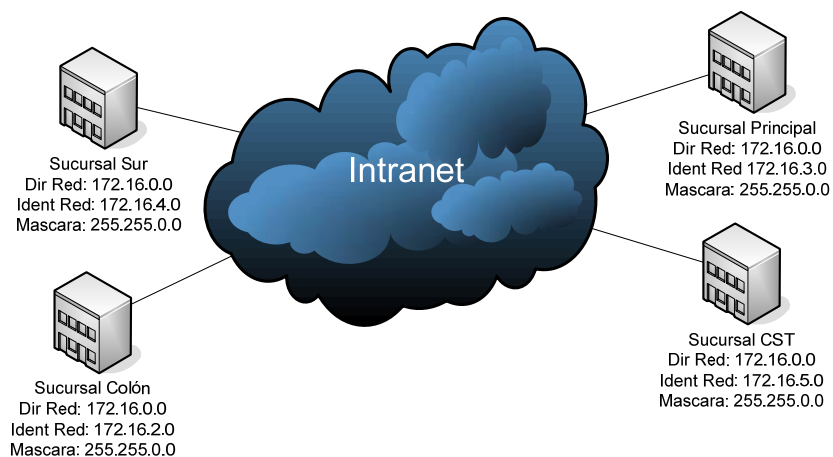


Figura 1-19: Direccionamiento IP Sucursales de Quito

En la red solo se tienen *switches* capa 2 y los ruteadores de banda ancha se los utiliza para el acceso de *Internet* y no hay otros ruteadores para interconectar las redes. Entonces si se segmentaría la red y no se cambiarían los equipos de conectividad, las redes de las sucursales quedarían aisladas.

Al tener un solo dominio de colisión para todas las sucursales de Quito, la red se vuelve lenta por: tormentas de *broadcast*, tarjetas de red dañadas o computadores infectados por *software* malicioso. Esto ha determinado que la red llegue a colapsar en algunas ocasiones.

1.4.1.2 Direccionamiento IP de las Sucursales de Guayaquil

El direccionamiento *IP* de las sucursales de Guayaquil se implementó con redes clase C. En Guayaquil se tienen dos sucursales, que son: Sucursal Mayor y Sucursal Sur.

Sucursal	Dirección de Red	Máscara	# de máquinas
Mayor	192.168.2.0	255.255.255.0	26
Sur	192.168.3.0	255.255.255.0	15

Tabla 1-24: Direccionamiento IP Sucursales de Guayaquil

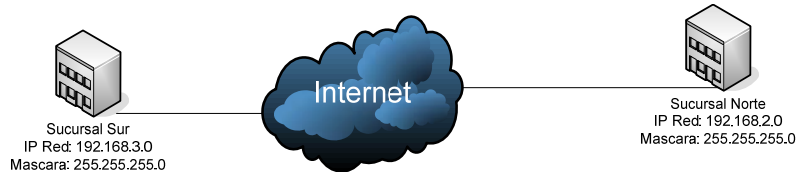


Figura 1-20: Direccionamiento IP Sucursales de Guayaquil

La Sucursal Mayor tiene asignada la dirección de red 192.168.2.0, que corresponde a una red clase C con máscara 255.255.255.0 y una capacidad máxima de 254 *host*, pero se tienen 26 *host* conectados a la red. El porcentaje de *host* instalados para el número máximo que permite la red es de alrededor del 10%, por lo que se recomendará realizar una segmentación por subredes para optimizar las direcciones *IP* disponibles.

En la Sucursal Sur se asignó la dirección de red 192.168.3.0, que corresponde a una red clase C con máscara 255.255.255.0 y puede alojar a 254 *host*. Existen 15 *host* conectados a la red, es decir que no se ocupa ni el 7% del número máximo que permite la red.

Las dos redes están totalmente aisladas, por lo que se quiere buscar una solución para interconectarlas y tener un direccionamiento *IP* coherente entre estas sucursales; además se va a interconectar las sucursales de Quito con las sucursales de Guayaquil, entonces se tiene que manejar un direccionamiento *IP* que guarde relación entre todas las sucursales.

1.4.2 DIRECCIONAMIENTO *IP* DE LOS ENLACES ENTRE SUCURSALES

Tecnomega posee enlaces de datos entre las sucursales de Quito; las sucursales de Guayaquil no tienen enlaces entre ellas. Tampoco se tiene un enlace Quito–Guayaquil. Los enlaces de Quito no utilizan direcciones *IP* porque son implementados con puentes inalámbricos; las direcciones *IP* configuradas en los *access points* sólo sirven para su administración.

1.4.2.1 Direccionamiento *IP* de los Enlaces entre las Sucursales de Quito

El direccionamiento *IP* utilizado para los enlaces entre las sucursales de Tecnomega Quito pertenece a redes clase C. El enlace entre la sucursal CST y la sucursal Sur se realiza mediante una dirección de red clase C: 192.168.10.0 con máscara 255.255.255.0.

El enlace entre la sucursal CST y la Colón corresponde a una red clase C: 193.169.10.0 con máscara 255.255.255.0. Esta dirección *IP* es una dirección pública, configurada en los equipos del enlace, pero éstos no van a ser administrados desde *Internet*; por lo que se debe cambiar estas direcciones para evitar conflictos con direcciones *IP* públicas utilizadas en *Internet*.

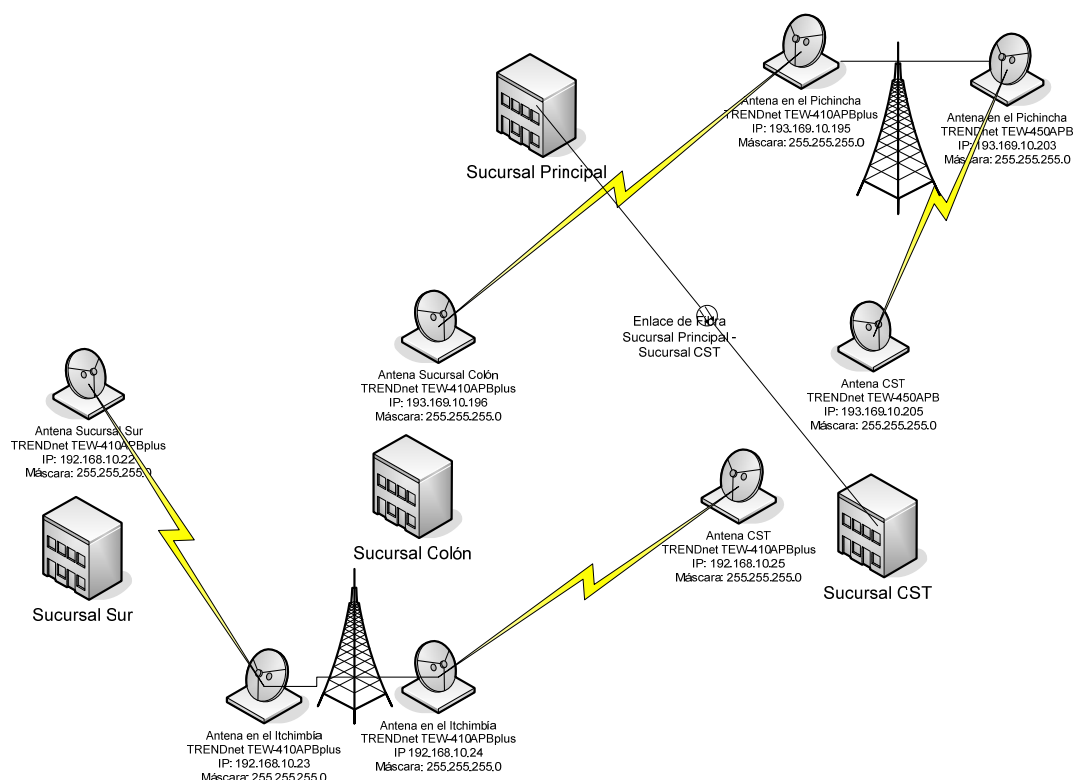


Figura 1-21: Direccionamiento *IP* de los enlaces de Quito

1.4.3 DIRECCIONAMIENTO *IP* PARA EL SERVICIO DE *INTERNET*

El direccionamiento *IP* para el servicio de *Internet* es dado por cada proveedor, mediante direcciones *IP* públicas que se incluyen en los paquetes contratados. Esto permite la interacción entre el servidor de *hosting* de la página *web* y el servidor de base de datos de cada sucursal para actualizar los datos de la página *web*, por medio de la réplica de la base de datos.

El proveedor de los servicios de *Internet* en Quito es Andinanet; incluye para cada sucursal en el servicio contratado dos direcciones *IP* públicas, que son: una para el módem *ADSL* y otra para un servidor *proxy* o un equipo para compartir el *Internet*, con la única excepción de la Sucursal Sur a la que se entrega una red clase C pública por ser un enlace punto a punto. A continuación se especifica el direccionamiento *IP* para el Servicio de *Internet*.

Sucursal	Dirección <i>IP</i> Red	Dirección <i>IP</i> Inicial Disponible	Dirección <i>IP</i> Final Disponible	Máscara de Red	Direcciones <i>IP</i> Disponibles
Principal	200.107.16.192	200.107.16.193	200.107.16.194	255.255.255.252	2
Colón	200.107.16.196	200.107.16.197	200.107.16.198	255.255.255.252	2
CST	200.107.16.128	200.107.16.129	200.167.16.130	255.255.255.252	2
Sur	190.11.27.0	190.11.27.1	190.11.27.255	255.255.255.0	254

Tabla 1-25: Direcciones *IP* Públicas para cada sucursal de Quito

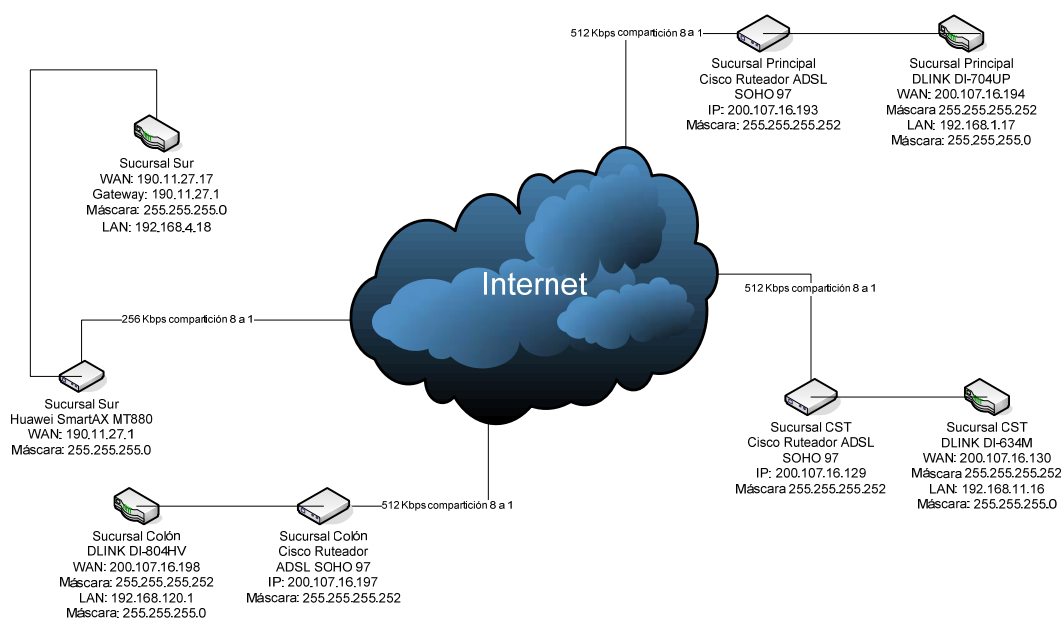


Figura 1-22: Esquema y Direccionamiento de salida a *Internet* en Quito

En Guayaquil se ha contratado los servicios del Grupo *TVCABLE*; el cual entrega 6 direcciones *IP* públicas con cada plan, para que el cliente las administre según su conveniencia.

Sucursal	Dirección <i>IP</i> Red	Dirección <i>IP</i> Inicial Disponible	Dirección <i>IP</i> Final Disponible	Máscara de Red	Direcciones <i>IP</i> Disponibles
Mayor	201.217.67.160	201.217.67.161	201.217.67.166	255.255.255.248	6
Sur	201.217.78.152	201.217.78.153	201.217.78.158	255.255.255.248	6

Tabla 1-26: Direcciones *IP* Públicas de las Sucursales de Guayaquil

En las Sucursales de Guayaquil se tienen cuatro direcciones *IP* por sucursal que no son utilizadas; estas direcciones *IP* pueden ser empleadas para: servidores que se puedan acceder desde *Internet*, telefonía *IP*, etc.

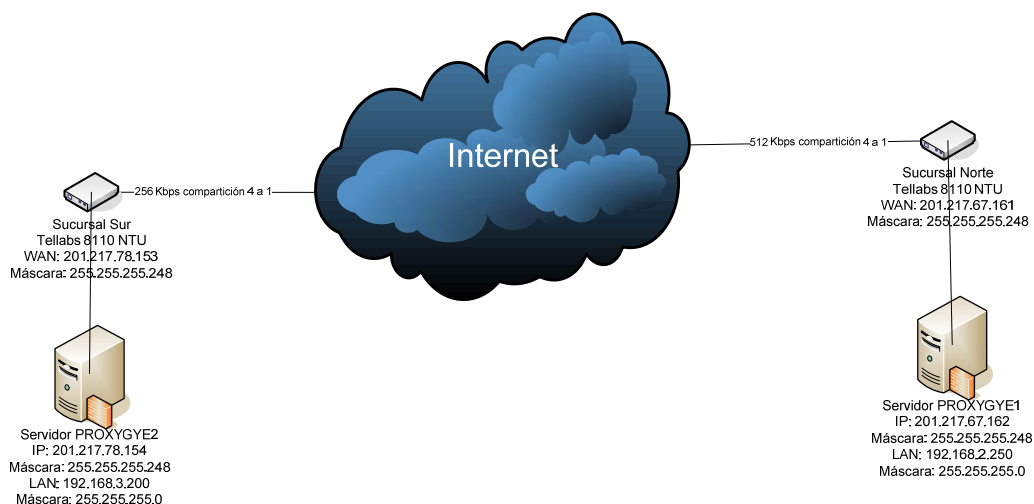


Figura 1-23: Esquema y Direccionamiento de la salida a *Internet* en Guayaquil

1.5 APLICACIONES DE LA *INTRANET*

La Intranet de Tecnomega fue desarrollada por el Departamento de Sistemas de la empresa. El proyecto nació hace un año y medio, con el objetivo de obtener reportes de la información almacenada en las bases de datos de cada sucursal.

El diseño e implementación de la Aplicación de la *Intranet* duró dos meses y se han ido adicionando reportes o consultas a medida que han surgido nuevos requerimientos. Todas estas nuevas funcionalidades se logran mediante nuevas consultas a las bases de datos de las sucursales, partiendo de la información ya almacenada; a veces se tiene que incrementar los campos en las tablas afines a la información o crear nuevas tablas.

Por medio de este sistema se tiene información rápida y confiable del *stock* de productos, ventas, etc. La *Intranet*, es muy utilizada por el personal de: Mercadeo, Gerencia, Ventas, Departamento Técnico y de Sistemas.

1.5.1 PERFILES DE USUARIO POR DEPARTAMENTO

Cada uno de los usuarios pertenece a un perfil por el área en la que trabaja:

- Perfil Gerencia
- Perfil Mercadeo
- Perfil Ventas
- Perfil Técnico
- Perfil Administrador

El perfil Gerencia tiene acceso a los siguientes servicios:

- Consulta de *Stock* por Agencias
- Consulta de *Stock* Global
- Consulta de Ventas por Artículo y por Agencia
- Consulta de Ventas por Artículo Global
- Consulta de Ventas por Vendedor
- Cuentas de Depósitos
- Lista de Precios
- Consultas de *RMA*³

³ *Return Merchandise Authorization (RMA)*: es utilizado en los distribuidores para transacciones de retorno de un producto por defectos de fabricación para repararlo o reemplazarlo.

- Consultas de Egreso de Garantía
- Consulta de Serie Global

El perfil del Departamento de Mercadeo tiene acceso a:

- Consulta de *Stock* por Agencias
- Consulta de Ventas por Artículo y por Agencias
- Consulta de Ventas por Artículos Globales

El perfil del Departamento de Ventas tiene acceso a:

- Consulta de *Stock* por Agencias

El perfil del Departamento Técnico tiene acceso a:

- Consulta de *RMA*
- Consulta de Egreso de Garantía
- Consulta de Serie Global

El perfil de Administrador, lo manejan las personas del Departamento de Sistemas y tienen acceso a las siguientes consultas:

- Consulta de *Stock* por Agencias
- Consulta de *Stock* Global
- Consulta de Ventas por Artículo y por Agencia
- Consulta de Ventas por Artículo Global
- Consulta de Ventas por Vendedor
- Cuentas de Depósitos
- Lista de Precios en Pantalla
- Lista de Precios en archivo
- Consultas de *RMA*
- Consultas de Egreso de Garantía
- Consulta de Serie Global
- Réplica *Web*

1.5.2 CONSULTAS Y SERVICIOS DE LA INTRANET

A continuación se muestran las pantallas de la *Intranet* de Tecnomega; la primera pantalla corresponde al ingreso mediante un nombre de usuario y una contraseña personal.



Figura 1-24: Pantalla de Acceso a la Intranet

1.5.2.1 Consulta de *Stock* de Productos por Sucursal

Esta consulta se la puede realizar en cada una de las sucursales, sólo se tiene que ingresar el código del producto para proceder con la misma.

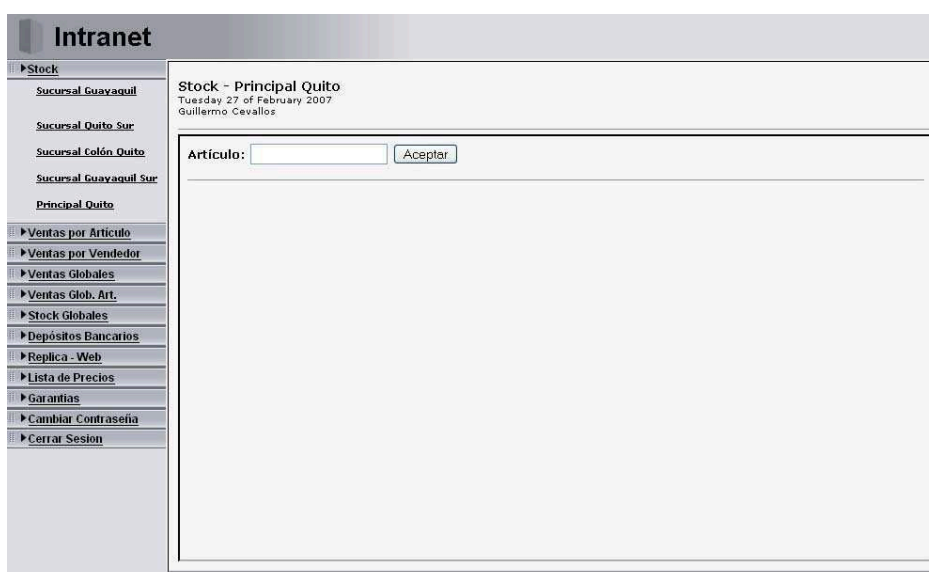


Figura 1-25: Pantalla de Consulta de *Stock* en Sucursales

La pantalla resultante de la consulta despliega la información del o los productos que se requieren, presentando las unidades producto existente y su precio.

Intranet

Stock - Principal Quito
Tuesday 27 of February 2007
Guillermo Cevallos

Artículo:

INVENTARIO SUCURSAL PRINCIPAL

Código	Artículo	Stock	Precio
MONLGSLL1730SSNT	MONITOR LG 17" L1730 SNT FLAT PANEL	1	276.00
MONLGLL1752TX	MONITOR LG 17" L1752TX FLAT PANEL	93	185.00
MONLGLL203WT-BA	MONITOR LG LCD 20" L203WT-BA	43	265.00
MONLGM3200CLK	MONITOR LCD 32" M3200C BLACK	3	1,500.00

Total: 4 Registro(s)

Figura 1-26: Pantalla de Resultados a la Consulta de Stock de Productos

1.5.2.2 Ventas por Artículo

Para realizar esta consulta se debe escoger la sucursal de la cual se quiere obtener la información e ingresar el producto; el sistema realiza una consulta a la base de datos de la sucursal elegida y se presenta la información.

Intranet

Ventas por Artículo - Principal Quito
Tuesday 27 of February 2007
Guillermo Cevallos

Fecha Desde: Feb 19 2007 Fecha Hasta: Feb 24 2007

Incluir Ventas a Tecnomega y Marcas:

Artículo:

VENTAS SUCURSAL PRINCIPAL
del 19/2/2007 al 24/2/2007

Código	Descripción	Cantidad	Subtotal	Dcto.	IVA	Total
MONLGLL17188BN	MONITOR LG 17" L17188 FLAT PANEL	154.00	27,546.00	0.00	236.28	27,782.28
MONLGLL1752TX	MONITOR LG 17" L1752TX FLAT PANEL	8.00	1,485.00	0.00	67.20	1,552.20
MONLGLL1952TX	MONITOR LG 19" L1952TX FLAT PANEL	1.00	229.00	0.00	0.00	229.00
MONLGLL203WT-BA	MONITOR LG LCD 20" L203WT-BA	2.00	530.00	0.00	31.80	561.80
Total		165.00	29,790.00	0.00	335.28	30,125.28

Figura 1-27: Pantalla de Ventas por Artículo

1.5.2.3 Ventas por vendedor

Es una consulta con carácter gerencial, esta consulta muestra por sucursales las ventas de un vendedor en un período determinado, se debe especificar la fecha de inicio y de fin para obtener la información.

Ventas por Vendedor - Principal Quito
Tuesday 27 of February 2007
Guillermo Cevallos

Fecha Desde: Feb 27 2007 Fecha Hasta: Feb 27 2007

Incluir Ventas a Tecnomega y Marcas

VENTAS SUCURSAL PRINCIPAL
del 27/2/2007 al 27/2/2007

Vendedor	Subtotal	Dcto.	IVA	Total
IRMA SILVA	4,144.50	41.79	364.95	4,467.66
JULIO ORTIZ	2,122.20	5.70	134.60	2,251.10
JHONNY PROCEL	1,519.60	30.31	126.58	1,615.87
JANETH SILVIA YANEZ	290.90	5.82	19.26	304.34
LUCIA VILLAREAL	462.00	0.00	55.44	517.44
MARITZA ALVAREZ	1,382.60	0.00	149.23	1,531.83
MIRIAM SANTOS	631.00	12.44	30.20	648.76
SARITA YANEZ	1,666.30	0.00	24.52	1,690.82
Total	12,219.10	96.06	904.78	13,027.82

Figura 1-28: Pantalla de Ventas por Vendedor

1.5.2.4 Ventas Globales

Es la consulta que resume las ventas en un período de tiempo que se han realizado, y entrega subtotales por sucursales a nivel nacional.

Ventas Globales -
Tuesday 27 of February 2007
Guillermo Cevallos

Fecha Desde: Feb 27 2007 Fecha Hasta: Feb 27 2007

Incluir Ventas a Tecnomega y Marcas

Agencia	Subtotal	Descuento	IVA	Total
AGENCIA PRINCIPAL	12,219.10	96.06	904.78	13,027.82
AGENCIA COLON	12,254.90	185.51	703.02	12,772.41
AGENCIA QUITO SUR	5,894.00	49.67	227.45	5,771.78
AGENCIA GUAYAQUIL	4,277.90	56.95	356.96	4,577.91
AGENCIA GUAYAQUIL SUR	1,411.85	9.59	111.58	1,513.84
Totales Generales:	35,757.75	397.78	2,303.79	37,663.76

Figura 1-29: Pantalla de Ventas Globales

1.5.2.5 Ventas Globales por Artículo

Es una consulta similar a la anterior la diferencia es que para esta consulta es indispensable ingresar el código del producto para obtener la información de las ventas de ese producto a nivel nacional.

Intranet

Stock
 Ventas por Artículo
 Ventas por Vendedor
 Ventas Globales
 Ventas Glob. Art.
 Stock Globales
 Depósitos Bancarios
 Replica - Web
 Lista de Precios
 Garantías
 Cambiar Contraseña
 Cerrar Sesión

Ventas Glob. Art. -
 Tuesday 27 of February 2007
 Guillermo Cevallos

Fecha Desde: Feb 27 2007 Fecha Hasta: Feb 27 2007 Incluir Ventas a Tecnomega y Marcas

Artículo: monlg Ver código artículo

Artículos	Principal	Colón	Quito Sur	Guayaquil Mayor	Guayaquil Sur	Total
MONITOR LG 17" L1718S FLAT PANEL	0	9	1	0	1	11
MONITOR LG 17" L1752TX FLAT PANEL	1	0	0	0	0	1
MONITOR LG 19" L1952TX FLAT PANEL	1	0	0	0	0	1
Totales Generales:	2	9	1	0	1	13

Figura 1-30: Pantalla de Ventas Globales por Artículo

1.5.2.6 Stock Global

En esta consulta se debe ingresar el código del producto para obtener la información correspondiente al *stock* del producto en cada sucursal.

Intranet

Stock
 Ventas por Artículo
 Ventas por Vendedor
 Ventas Globales
 Ventas Glob. Art.
 Stock Globales
 Depósitos Bancarios
 Replica - Web
 Lista de Precios
 Garantías
 Cambiar Contraseña
 Cerrar Sesión

Stock Globales -
 Tuesday 27 of February 2007
 Guillermo Cevallos

Artículo: monlg Ver código artículo

Artículos	Principal	Colón	Quito Sur	Eye Mayor	Eye Sur	Total	Precio
MONITOR LCD TV 32" 32LX2R	0	0	0	1	0	1	1,589.00
MONITOR LG 17" L1718S FLAT PANEL	0	2	5	78	39	124	179.00
MONITOR LG 17" L1730 SHT FLAT PANEL	1	0	0	0	0	1	276.00
MONITOR LG 17" L1752TX FLAT PANEL	93	301	80	176	54	704	185.00
MONITOR LG 19" L1950SN FLAT PANEL	0	0	1	0	0	1	236.00
MONITOR LG 19" L1952TX FLAT PANEL	0	0	0	5	2	7	229.00
MONITOR LG LCD 20" L203WT-8A	43	71	10	21	4	149	265.00
MONITOR LCD 32" M3200C BLACK	3	1	1	0	0	5	1,500.00
Totales Generales:	140	375	97	281	99	992	

Figura 1-31: Pantalla de Stock Global

1.5.2.7 Depósitos Bancarios

Este servicio sirve para consultar el estado de cuenta en los bancos, para verificar depósitos de clientes especialmente de provincia que realizan sus pagos por depósitos a cuenta o transferencia. No se dispone de una pantalla para este servicio de la *Intranet*, por motivos de seguridad y sigilo bancario.

1.5.2.8 Réplica Web

Este servicio está disponible solo para usuarios del perfil administrador, y realiza una réplica de las bases de datos de todas las sucursales para actualizar la información de la página web. Este procedimiento se lo realiza todos los días manualmente, se tiene un proyecto para realizar las réplicas en tiempo real pero todavía está en fase de pruebas.

1.5.2.9 Listas de precios

Este servicio tiene dos opciones que son:

- Lista de precios en pantalla, esta consulta muestra la lista de productos existentes en las sucursales con sus respectivos precios.

CODIGO	ACCESORIOS	PRECIO	STOCK
ACCADUAWA-9DB1	ANTENA 9DB1 ADVANTEK WI-FI HIGH PERFORMANCE 3M	58.00	3
ACCADVSKVAUSB	SKYBOX ADVANTEK COMUNICADOR INTERNET USB	39.00	5
ACCAPCCARUNIP0D	CARGADOR UNIVERSAL DE PODER NOTEBOOK	79.00	39
ACCAPCP0INV350W	POWER INVERTER APC PORTABLE 350W 2 OULET	56.00	1
ACCCECB0120	BLUETOOTH CBD-120 V2.0 USB 150MTS.	22.00	3
ACCCECB0220	BLUETOOTH CBD-220 V2.0 USB 80MTS.	20.00	2
ACCDLKB0T122	ADAPTER USB BLUETOOTH SIG 1.2	24.00	3
ACCLGXAP42WA50M	WALL MOUNTLG LG 42" Y 50"	69.00	23
ACCLGXL3200STBK	STAND L3200 BLACK MONITOR FLATRON	34.00	6
ACCLGXPPORCDS	PORTA CDS LG	3.00	23
ACCXXRECHKIT	RECARGADOR BATERIAS KIT 120V	16.00	1
ADAPSPS180TMLU	ADAPTADOR EPSON PS-180 Pn:C825343	28.00	2
ADAXXPS2LUSB	ADAPTADOR PS/2 - USB	1.00	54
ADAXXUSB/PS2	ADAPTADOR USB - PS/2	1.00	178
CABDLKXVM-CB	KIT CABLE KVM	10.00	12
CABXXXIDE	CABLE IDE (BUS DE DATOS)	1.00	216
CABXXXIDE-SRATA	CABLE SERIAL ATA	2.00	569
CABXXXIMPPAR	CABLE IMPRESORA PARALELO	1.00	17
CABXXXLOCK	CABLE LOCK DEPCON	36.50	2
CABXXXPODER	CABLE DE PODER	1.00	24
CABXXXSDATA	CABLE IDE SERIAL DATA 7PIN,7PIN 0.5MTS	1.50	1068
CABXXXUSBTYA	CABLE USB SLOT TYPE A	0.90	1388
CAJXXXDINMET	CAJA DINERO METALICA	92.00	25
PODXXXMM0460M	DISCETA DL 4MB,300,MB,4.4,512K	16.00	123

Figura 1-32: Pantalla Listas de Precios de la *Intranet*

- Lista de precios en archivo, es un procedimiento para obtener un archivo con lista de productos existentes con sus precios.



Figura 1-33: Pantalla de Descargar el Archivo de Lista de Precios en Excel

1.5.2.10 Garantías

Sirve para hacer: ingresos y egresos de garantía, así como el histórico de productos. A continuación se detallan estos tres submenús de garantías:

- Ingreso de Garantía, se puede consultar los productos que han ingresado por garantía. La consulta puede hacerse:
 - Mediante el número de serie del producto, para obtener información del producto en garantía;
 - Se puede ingresar el código del artículo y especificar el período de consulta; se obtienen todos los productos con ese código;
 - Se puede ingresar una marca de las que comercializa Tecnomega para obtener los resultados deseados en un período específico; se muestran estadísticas de los productos en garantía de esa marca elegida.
 - Consultar ingresando el código de cliente para obtener los productos que han ingresado por garantía.

Figura 1-34: Pantalla Ingreso de Garantías (RMA)

Figura 1-35: Pantalla Ingreso de Garantías (RMA) 2

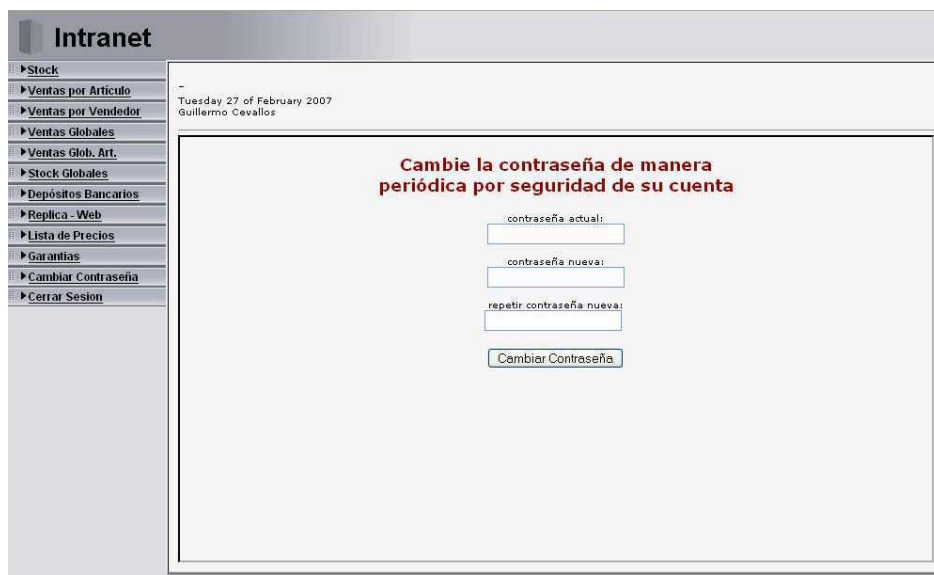
- Egreso de *RMA*, cuando se entrega al cliente el producto que ingresó por garantía se genera un egreso de *RMA* donde se especifica: el técnico que atendió el caso, el tiempo de solución del problema y la solución del mismo. Toda esta información se almacena en la base de datos para tener un historial del producto. (No se tiene una pantalla de este servicio en la *Intranet*)

- Histórico Serie, se refiere al historial que lleva un producto desde que ingresa a las bodegas de Tecnomega, se registra a quién se vende el producto y si se ha ingresado por garantía y qué solución se le dio para cubrir la garantía, así se tengan varios ingresos por garantía.

Este servicio de la *Intranet*, es la base para el servicio de la página *web* Garantías en línea, donde los clientes pueden consultar el estado de los productos que han ingresado por garantía, donde se especifica el tiempo estimado de solución, el técnico encargado, etc.

1.5.2.11 Cambiar Contraseña

Todos los usuarios pueden cambiar su clave el momento que lo deseen; adicionalmente por seguridad deben cambiarla periódicamente.



The screenshot shows a web interface for an Intranet. On the left is a vertical navigation menu with the following items: Stock, Ventas por Artículo, Ventas por Vendedor, Ventas Globales, Ventas Glob. Art., Stock Globales, Depósitos Bancarios, Replica - Web, Lista de Precios, Garantías, Cambiar Contraseña, and Cerrar Sesión. The main content area has a header with the date 'Tuesday 27 of February 2007' and the name 'Guillermo Cevallos'. Below the header, a red heading reads 'Cambie la contraseña de manera periódica por seguridad de su cuenta'. The form contains four input fields: 'contraseña actual:', 'contraseña nueva:', 'repetir contraseña nueva:', and a 'Cambiar Contraseña' button.

Figura 1-36: Pantalla para Cambio de Claves de Usuarios

1.6 SERVICIOS DEL SITIO *WEB*

La página *web* ofrece información de la empresa y servicios en línea para sus clientes. En la página inicial se tiene:

- Información sobre la compañía, una pequeña descripción sobre sus actividades, también se incluye la misión, visión y los valores.
- *Login*, para usuarios registrados de la página *web*; adicionalmente se permite registrar nuevos usuarios que no se han registrado para los servicios en línea, pero son ya clientes de Tecnomega.
- *Stock* y Productos, se muestra el detalle de las marcas de los productos; adicionalmente se muestra su disponibilidad en cada una de las sucursales y la última fecha en que se actualizó este reporte.
- Promociones, se detallan las promociones vigentes.
- Noticias, es la parte de la página donde se dan a conocer los nuevos productos, se especifican sus características técnicas y posibles usos.
- CST y garantías en línea; el Centro de Servicio Técnico (CST) presenta el estado de los productos que han retornado por garantía, el tiempo de solución, cómo se dará solución al reclamo de garantía y el nombre del técnico encargado.
- Políticas de Garantía de productos y sus respectivos tiempos de garantía; se especifican las marcas y la modalidad de las garantías, especialmente el tiempo de garantía de los productos.
- Contáctenos, se compone de un formulario de contacto para enviar un correo electrónico, se da la opción de dirigirlo a varias áreas de la empresa según sea el contenido del mensaje. Adicionalmente, se muestran los números de teléfono de las sucursales de la empresa, así como sus direcciones y ciudades donde se encuentran ubicadas.
- Eventos, en esta sección se publican las fotos de los últimos eventos organizados por Tecnomega a nivel nacional.



Figura 1-37: Página Inicial www.tecnomega.com

1.6.1 REGISTRO DE USUARIOS DE LA PÁGINA WEB

Los clientes de Tecnomega que deseen acceder a los servicios en línea, se pueden registrar por medio de la página web. Para registrarse se necesita el RUC de la empresa; cuando se valida el RUC se ingresan los datos del representante legal. Una vez registrado el cliente se le envía un *email* para informarle que el registro ha sido exitoso, y se incluye la clave del usuario.

Para ingresar a la página web se debe ingresar el RUC de la empresa y la clave, luego se valida el usuario y si es válido se muestra una pantalla de todas las sucursales de Tecnomega en donde tiene un código activo.

La página web tiene información específica de cada sucursal en lo referente a disponibilidad de productos, por lo que se debe escoger a qué sucursal se quiere ingresar.



Figura 1-38: Página de *Login* del Usuario de una Sucursal

1.6.2 SERVICIOS WEB

Los servicios en línea están disponibles sólo para usuarios registrados. Para usuarios no registrados se tiene una parte de información de la empresa, como: visión, misión y valores; productos nuevos (pero no se muestran precios ni disponibilidad); eventos organizados por la empresa; entre otros. A continuación se muestran los servicios en línea de la página *web*.

- Pedido con lista de precios en modo pantalla
- Pedido con lista de precios en modo impresora
- Productos disponibles
- Lista de precios en formato *Microsoft Excel*
- Productos llegados
- Garantías en línea
- Envíos de mercadería

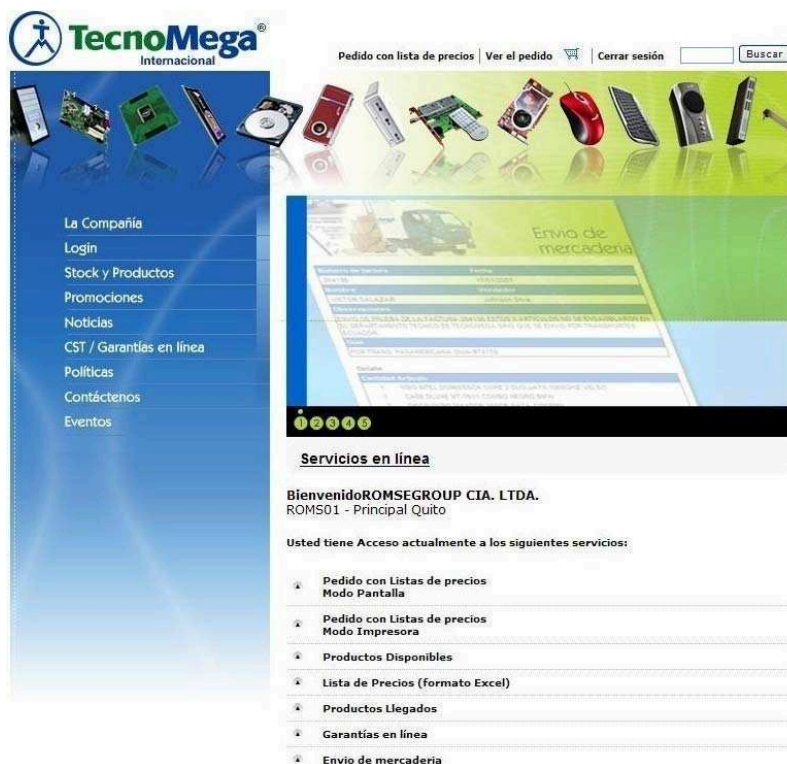


Figura 1-39: Servicios de la Página Web

1.6.2.1 Pedido con Lista de Precios Modo Pantalla

Muestra la lista de precios de productos y si se escoge un producto se lo adiciona a la canasta de compras para hacer un pedido.

1.6.2.2 Pedido con Lista de Precios Modo Impresora

Se despliega una lista de precios de los productos para imprimirla.

1.6.2.3 Productos Disponibles

Se organizan los productos disponibles por marca o por tipo; para hacer más fácil la búsqueda, se debe seleccionar un producto para obtener información sobre su disponibilidad y en qué sucursal lo tienen.

[Pedido con lista de precios](#) | [Ver el pedido](#) | [Cerrar sesión](#) |

TecnoMega
 Internacional

La Compañía
 Login
 Stock y Productos
 Promociones
 Noticias
 CST / Garantías en línea
 Políticas
 Contáctenos
 Eventos

Productos

Ver en modo de lista de precios >

Marcas	Líneas
General	Accesorios
3 Com	Bandeja Impresora
Advantek Networks	Cámaras Digitales
Amd	Chasis
Apc	Chasis Super Power
Asrock	Celulares
Benq	Computadores
Biostar	Procesadores
Cnet	Faxes
Codegen	Flash Memory
Corsair	Fuente De Poder
Creative Lab	Discos Duros

Figura 1-40: Página de Productos Disponibles por Marcas o Líneas

1.6.2.4 Lista de Precios (Formato *Microsoft Excel*)

El formato de lista de precios para imprimir. A los clientes registrados en la base de datos, se les envía un *email* periódicamente de la lista de precios, donde se tiene un enlace para descargar esta lista de precios.

1.6.2.5 Productos Llegados

Es una lista de precios de los productos que han llegado en el último embarque. A los clientes registrados en la base de datos, se les envía un email con la lista de precios de productos llegados, cada vez que llega un embarque.

1.6.2.6 Garantías en línea

Para acceder a este tipo de consultas de garantías en línea se debe ingresar el número de *RMA* del producto ingresado por garantía y el año de compra.

Figura 1-41: Página de Consultas de Garantías

1.6.2.7 Envío de Mercadería

Es un servicio muy útil con el cual se puede dar seguimiento a los envíos de mercadería a domicilio, ingresando el período de fechas del envío.

Figura 1-42: Página de Consulta de Envío de Mercadería

1.6.3 ESQUEMA PARA CONSULTAS ENTRE SUCURSALES

Para hacer posible las consultas del *stock* de cada sucursal se han establecido enlaces lógicos o físicos, por medio de las direcciones *IP* públicas de cada sucursal. Las sucursales de Quito se conectan por enlaces inalámbricos privados, las consultas de las bases de datos entre las sucursales de Quito utilizan estos enlaces.

Las consultas para las sucursales de Quito se las realiza de la siguiente manera: se hace el requerimiento de consulta y se envía al Servidor *Web* de la Sucursal CST, éste a su vez ubica al servidor de cualquiera de las sucursales de Quito para reenviar el requerimiento; luego el Servidor de Base de Datos procesa la consulta y entrega el resultado al Servidor *Web* del CST y éste lo devuelve al Servidor de la Página *Web* de Tecnomega, logrando el usuario visualizar el resultado de su consulta.

Las consultas de las sucursales de Guayaquil, se realizan por medio de Internet sin levantar una *VPN* para la seguridad de la información; se utiliza este procedimiento por la falta de enlaces entre las sucursales de Guayaquil.

El mecanismo para las consultas de *stock* de Guayaquil es de la siguiente manera: la página *web* genera el requerimiento y lo envía a la dirección *IP* registrada, el Servidor *Web* del CST recoge el requerimiento y lo transmite al Servidor de Base de Datos de la sucursal, procesa el requerimiento y devuelve la respuesta al Servidor *Web* del CST y éste devuelve el dato al Servidor *Web* de *Yahoo*.

En base a estas consultas se genera la aplicación de la *Intranet* para obtener información de ventas, *stock*, etc. Esta *Intranet* les sirve a los gerentes de cada departamento para ver los resultados de sus empleados.

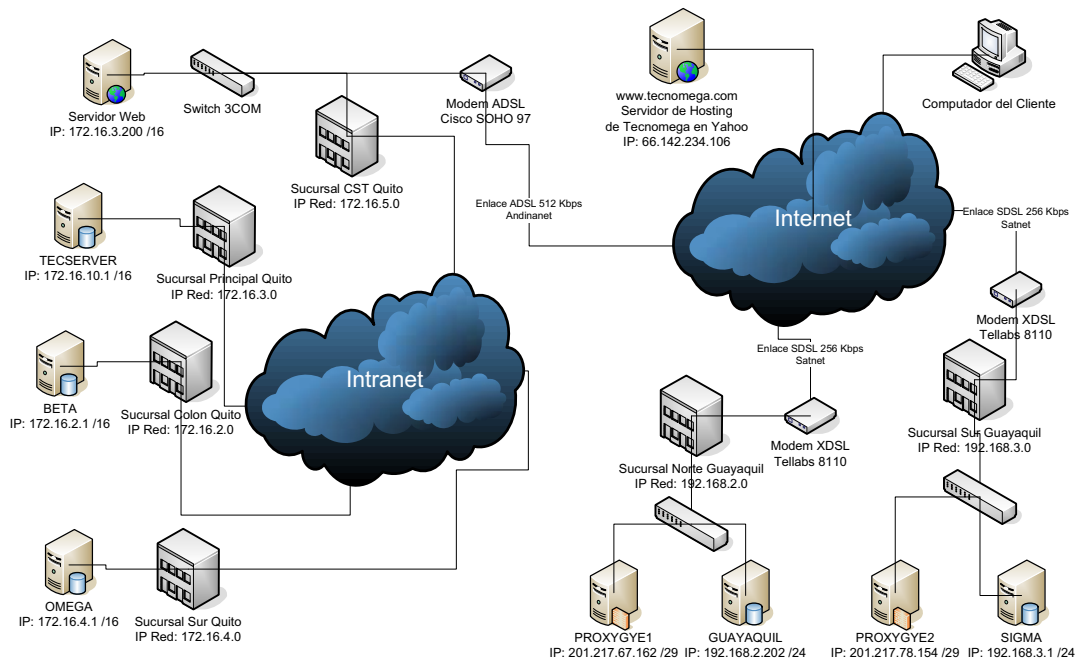


Figura 1-43: Esquema Físico para Consulta de Stock en las Sucursales

Las consultas que se hacen en la *Intranet* tienen la misma lógica que las consultas de *stock* para la página *web*.

1.7 ESQUEMAS DE SEGURIDAD DE LA RED

Los esquemas de seguridad de la red son de mucha importancia en este tiempo que es la era de la información; se busca proteger la información empresarial, como por ejemplo: información contable, bases de datos de clientes, inventario de bodega, etc. La pérdida de este tipo de información puede impedir la operación de la empresa.

La seguridad de la red en caso de alguna amenaza da una ventaja competitiva a la empresa, ya que podrá seguir operando aun cuando algún problema ocurra. La continuidad en la operación de la empresa en estos casos genera y mantiene la confianza de sus clientes, lo que se ve reflejado en el incremento de sus ventas y clientes.

La seguridad de la red no es algo que se pueda notar cuando se tiene un correcto funcionamiento del sistema, es decir, no mejora el rendimiento del sistema. La seguridad se notará cuando la red sea víctima de un ataque e impida que el ataque afecte o disminuya su impacto.

Un sistema de seguridad para red necesita: prevención, éste es un proceso continuo donde se debe utilizar *hardware* y *software* para implementar el sistema de seguridad; detección, por medio de *hardware* o *software* se puede detectar cuando la red está siendo atacada; respuesta, para responder a un ataque se debe elaborar un plan de contingencias mediante el establecimiento de políticas de seguridad.

En Tecnomega no se ha puesto mucho interés en la seguridad de la red, hoy en día se tienen problemas de fuga de información, se necesita incluir seguridades en la red para mitigar o eliminar este grave problema. Hasta la fecha no se tienen políticas de seguridad en la empresa; el diseño de estas políticas es imprescindible para disminuir las vulnerabilidades y asegurar la información empresaria.

1.7.1 SEGURIDAD LÓGICA

La seguridad lógica está muy descuidada en Tecnomega y en la mayoría de las empresas en el Ecuador, en las que no se tiene un cambio visible cuando se implementan seguridades en su red.

La seguridad lógica se la dividió en categorías para su análisis:

- Direccionamiento *IP* y Segmentación de la red
- Configuración de Equipos
- Manejo de Claves
- *VPN*

1.7.1.1 Direccionamiento *IP* y Segmentación de la Red

El direccionamiento *IP* implementado en la empresa no ayuda a implementar seguridades, ya que no existe segmentación de la red, todos los usuarios pueden ingresar y observar toda la red. La segmentación de la red serviría para implementar el esquema de seguridad dividiendo la red según un criterio que puede ser por departamentos o sucursales; este criterio debe ser escogido teniendo en cuenta el tráfico de datos a los servidores y a cuáles servidores se necesita el ingreso de cada departamento.

El esquema de seguridad que se tiene al momento es seguridad por obscuridad, porque para ingresar a la red se necesita conocer la dirección *IP* y la máscara. Este tipo de seguridad no es apropiada para la empresa ya que dentro de la misma existen personas que tienen conocimiento sobre computadores y redes, pudiendo consumir un ataque por algún motivo. Los ataques más peligrosos son los ataques internos y los más comunes.

Para tener un sistema de seguridad robusto se debe segmentar la red buscando un direccionamiento *IP* que satisfaga las necesidades de la empresa y que los usuarios tengan acceso exclusivamente a las aplicaciones y a los servidores que sea necesario.

Para unir las redes que así lo necesiten se deben usar ruteadores y/o *switches* capa 3, programando Listas de Control de Accesos donde se limite el acceso de ciertas direcciones *IP* a algunas redes restringidas e instalando *Firewalls* Físicos para tener registros de los usuarios que ingresan (alcanzando Contabilidad y Autenticación); adicionalmente se deberá tener un Sistema de Detección o Prevención de Intrusos para que alerte cuando se tenga un comportamiento sospechoso y según el caso se tomen acciones contra el ataque en curso.

1.7.1.2 Configuración de Equipos de Conectividad

En los equipos de conectividad como: ruteadores, *access point* se ha dejado la configuración por defecto, sin personalizar las opciones de seguridad que traen estos equipos. Ésta es una vulnerabilidad que debe ser corregida lo más rápido posible para evitar futuros ataques. Al dejar la configuración por defecto puede existir interferencia en el caso de equipos inalámbricos, porque muchos usuarios solo cambian algunas configuraciones básicas para que funcionen los equipos pero no se realiza una configuración referente a la seguridad.

Para la red inalámbrica no se ha diseñado un esquema de seguridad, no se han incorporado claves de acceso para autenticación de los usuarios; no se ha implementado un esquema de seguridad robusto para autenticación *WPA2* con un servidor *RADIUS* para que cada uno de los usuarios tenga su propia clave. Tampoco se tiene restricción de ingreso de equipos por direcciones *MAC* o no difusión del *SSID* que son esquemas de seguridad mínimos para una red inalámbrica.

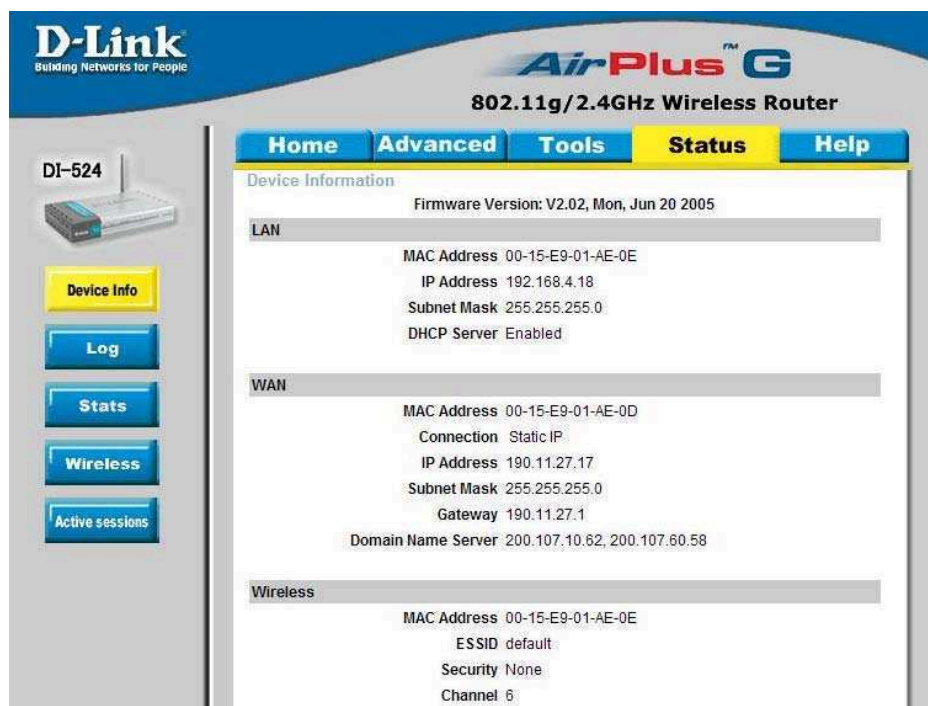


Figura 1-44: Pantalla de Configuración Ruteador Inalámbrico por defecto

Como se puede ver en la captura de pantalla de uno de los ruteadores inalámbricos, no se ha configurado la seguridad en el equipo; el *SSID* tampoco se lo ha cambiado del que viene configurado por defecto y por ultimo no se ha realizado una prueba de campo para analizar las señales en el medio inalámbrico y configurar el canal de frecuencia del equipo.

Este descuido o desconocimiento crea una vulnerabilidad, que puede ser aprovechada por personas mal intencionadas para robar información o ingresar a la red y causar daños al sistema. Éste es solo un ejemplo de las vulnerabilidades que tiene la red de Tecnomega a nivel lógico.

Los equipos no tienen una correcta gestión de actualizaciones de *firmware* o *software*, según sea el caso. Los fabricantes de los equipos de conectividad, ponen a disposición actualizaciones de *firmware* o *software* para corregir: vulnerabilidades encontradas, problemas de estabilidad, adicionar algunas funcionalidades o manejos de protocolos nuevos. Pero esto no es tomado en cuenta por los técnicos de la empresa, es suficiente que funcione el equipo y no se lo actualiza.

El *software* de los dispositivos de red, computadores, servidores; tienen sistemas operativos que deben actualizarse para ser más robustos contra ataques, todos los meses están disponibles actualizaciones de seguridad referentes a vulnerabilidades encontradas. Éstas deben ser instaladas para corregir huecos de seguridad, para que los atacantes no se aprovechen esto y hagan daño.

Existen programas como el *Microsoft ISA Server*, para manejo de actualizaciones para redes, que por medio de *Web Cache* se mejoran la administración de la capacidad de *Internet*; al tener en *Cache* almacenadas todas las páginas frecuentemente visitadas, se hace ágil su visualización y la optimización de la capacidad de *Internet*. Todavía no se ha implementado ningún sistema de *web cache* para manejar las actualizaciones en empresa.

Los programas de antivirus y anti-espías, *firewall*, etc., deben actualizarse periódicamente. La empresa tiene un sistema de antivirus corporativo instalado en cada servidor de cada sucursal. Muchos *software* maliciosos, virus o espías pueden hacer colapsar la red al enviar archivos basura e inundar la red; el tipo de antivirus para redes corporativas tiene mecanismos de Detección de Intrusos avanzados que previenen ataques y alertan al sistema de seguridad para que se tome alguna acción.

1.7.1.3 Cambio de Claves de Acceso

Los equipos de red como ruteadores, *access points* y equipos de computación no tienen una política de seguridad de cambio de claves periódico; algunos equipos no tienen clave de acceso o se deja la clave por defecto.

Los atacantes que han configurado este tipo de equipos saben cuáles son las contraseñas por defecto y lo que primero hacen es probar estas contraseñas para tratar de entrar a la red. No se deben utilizar contraseñas fáciles de imaginar o asociar con la empresa, se deben utilizar contraseñas robustas de más de ocho caracteres entre letras mayúsculas, minúsculas y números.

Los cambios de claves de acceso a los equipos de conectividad deben cumplir con la política de seguridad que se establezca en la empresa. Este procedimiento se debe realizar periódicamente, según el tiempo establecido que puede ser de un mes, dependiendo de las necesidades y en relación a la importancia del equipo.

Para acceso a servidores o equipos de red de mayor importancia se pueden instalar controles de acceso biométricos, como por ejemplo: con huella digital, iris del ojo o la forma de la mano, etc.; dependiendo de los costos que estos impliquen y el costo de lo que se quiere proteger se deberá escoger un sistema de control de acceso.

1.7.1.4 Redes Privadas Virtuales (VPN)

Al momento, en la empresa no se tienen implementadas VPN en ningún enlace entre sucursales ni a través de *Internet*. En los enlaces entre las sucursales la información se transmite en texto plano, sin ningún esquema de encriptación y no se ha implementado ningún esquema de seguridad.

En los enlaces a través de *Internet*, que se utilizan para las consultas de la *Intranet* en las sucursales de Guayaquil, no se ha implementado para eso una VPN entre la Sucursal CST y el Servidor de *Hosting* de *Yahoo* o las Sucursales de Guayaquil y el Servidor de *Hosting* de *Yahoo*. Éste es un punto vulnerable para que algún espía robe la información de clientes o del *stock* y lo utilice para robarse clientes o para fines de competencia desleal.

La implementación de VPNs en todos los enlaces que tiene la empresa en *Internet* y los enlaces entre las sucursales es primordial para dar mayor seguridad a la información que viaja por los mismos. La información corre riesgo, así sea transportada por enlaces privados o por *Internet*, por esto debe transportarse encriptada en una VPN.

Las VPNs se pueden levantar desde algunos dispositivos de red y servidores, tales como: *firewalls*, ruteadores, servidores o computadores con programas para levantar y terminar VPNs; se debe escoger una alternativa según el caso específico desde donde se quiera tener la VPN.

1.7.2 SEGURIDAD FÍSICA

La seguridad física de los equipos de conectividad, servidores, etc., es muy importante ya que la red puede ser muy segura lógicamente, pero físicamente se pueden robar un servidor, un disco duro o los CDs de respaldo de una base de datos.

1.7.2.1 Cuartos de Telecomunicaciones

Todos los equipos de conectividad deben ser ubicados en cuartos de telecomunicaciones para su seguridad física, en la empresa esto no se cumple en algunas de las sucursales de Quito. Por ejemplo, en la Sucursal Principal, se tiene un *rack* sin armario el cual está ubicado junto a las gradas y al baño; ha sucedido que niños han desconectado los equipos, perdiéndose la conectividad entre las sucursales o entre los computadores.

En la Sucursal Principal se ha improvisado ubicar *switches* o *hubs* en oficinas por falta de puntos de red, esto va en contra de toda norma de seguridad, ya que se pone a disposición de cualquier persona más puntos de red y el equipo no está en un sitio seguro; cualquier persona puede conectar un computador a este *switch* y entrar a la red sin problema.

Los cuartos de telecomunicaciones deben tener un control del acceso manejado por medio de tarjeta magnética, lector de huella digital, lector de la forma de la mano, etc. Por lo general el área de servidores es restringida y solo tiene acceso el personal autorizado para esto. En la empresa no se tienen estas medidas para el control de acceso a sitios donde están instalados los equipos de conectividad y servidores.

Las nuevas sucursales fueron construidas a medida de las necesidades como lo son las dos sucursales de Guayaquil y la sucursal Colón de Quito. En estas sucursales se puede notar que se tiene mejor ubicado los servidores y equipos de conectividad, en un cuarto de telecomunicaciones, que se encuentra en un lugar no tan accesible.

El cableado de la red debe estar asegurado dentro de las paredes o en canaletas para dificultar el acceso, evitando que un atacante pueda acceder a estos cables para conectarse a la red. Estos cables deben estar bien sujetos y fijados directamente, del *patch panel* del cuarto de telecomunicaciones al *face plate* donde se conecta el usuario.

1.7.2.2 Equipos de Conectividad para Seguridades de la Red

Los equipos de conectividad en especial *switches*, que tiene la empresa son equipos básicos no administrables, que no disponen de funciones para Listas de Control de Accesos, manejo de Calidad de Servicios, restricción de direcciones *MAC* para ingresar a la red.

Todas estas bondades de equipos más robustos ayudan a implementar un sistema de seguridad, por lo que en el rediseño de la red se dimensionarán los equipos y especificarán las características que se necesitan para adquirir equipos que cumplan con las expectativas de seguridad.

Los equipos que tienen administración como los ruteadores de banda ancha cableados o inalámbricos pueden incorporarse a un esquema de seguridad básico, pero no están configurados para esto. Estos equipos manejan esquemas de seguridad básicos, que no necesariamente son lo que necesita una empresa del tamaño de Tecnomega.

La seguridad inalámbrica implementada en la empresa es *WPA*, la cual no es aconsejable para empresas, porque en *Internet* y en revistas como *PCMagazine* del mes de Septiembre de 2007, se habla que los esquemas de encriptación para redes inalámbricas *WEP* y *WPA* pueden ser violentados en menos de 10 minutos con un computador estándar.

La seguridad inalámbrica a implementarse es *WPA2 Enterprise*, ya que el esquema de seguridad inalámbrica más recomendable para una empresa, donde la autenticación realiza un servidor *RADIUS* externo. El servidor *RADIUS* puede manejar esquemas de autenticación por medio de nombres de usuario y contraseñas o por certificados digitales en el servidor y/o en el cliente.

En la red actualmente no se manejan *Firewalls*, Sistemas de Detección de Intrusos o Sistemas de Prevención de Intrusos, por esta razón y por la falta de un Antivirus Corporativo la red se satura y se tiene mucho tráfico basura.

En el rediseño de la red se deben incluir equipos que manejen autenticación de usuarios de la red cableada e inalámbrica, este sistema de autenticación debe estar ligado a un dominio corporativo donde se almacenan los nombres de usuario y sus respectivas contraseñas de acceso.

Se deben adquirir *switches* capa 3 para la interconexión de las redes de las sucursales; *firewalls* para proteger los servidores de los atacantes y ruteadores para la segmentación de la red. Todos estos equipos deben cumplir con las especificaciones que se obtengan del producto de este presente Proyecto de Titulación.

CAPÍTULO 2
ANÁLISIS DE
REQUERIMIENTOS
Y ALTERNATIVAS
TECNOLÓGICAS

2 ANÁLISIS DE REQUERIMIENTOS Y ALTERNATIVAS TECNOLÓGICAS

2.1 ANÁLISIS DE REQUERIMIENTOS

Este análisis de requerimientos se lo realizó en base a las conversaciones mantenidas con el personal del Departamento de Sistemas, el Gerente Técnico, y el personal Administrativo de Tecnomega. Cada uno de los departamentos determinó sus requerimientos de la red; muchas de las personas están preocupadas por la fuga de información de los servidores y no se ha podido determinar su origen, por la falta de un esquema de seguridad en la empresa.

La seguridad en la *Intranet* Corporativa de una empresa es indispensable, porque así mantiene su ventaja competitiva. La competencia es muy dura entre las empresa Mayoristas de Computación porque tienen una estrecha diferencia de precios; por ello esta información debe ser solo para clientes y no para la competencia. En consecuencia la información de los clientes registrados en la empresa debe ser guardada con sigilo.

Sin ser menos importante, se busca la integración de todas las sucursales en una red, donde se pueda tener un dominio interno para ejecutar aplicaciones en la *Intranet*, Antivirus Corporativos y sacar provecho de las bondades que ofrece el dominio corporativo para el control de acceso de usuarios registrados. Adicionalmente se ganará el registro de la actividad de los usuarios en los servidores de la empresa.

La integración de las comunicaciones de la empresa es muy importante para disminuir costos; hoy en día para comunicarse con otra sucursal de la empresa se tiene que llamar desde una línea de Andinatel (en Quito) o una de Pacifictel (en Guayaquil), teniendo que pagar por cada llamada realizada.

Con la telefonía *IP* integrada en todas las sucursales de la empresa se reducirán las planillas telefónicas, porque ya no se tendrá que llamar a números de las operadoras telefónicas para mantener una conversación entre personal de la empresa dentro y fuera del país.

El servicio de *Internet* contratado por la empresa no satisface las necesidades de los usuarios, el problema radica en que no se ha realizado un estudio donde se determine la capacidad necesaria y las características del servicio que se necesita contratar. Adicionalmente, se tiene mucha desorganización en contratar los servicios de *Internet* porque no se tiene conocimiento de las características de los servicios contratados, lo único que se ha tomado en cuenta para contratar uno u otro servicio es el precio.

La administración de la red es una tarea muy difícil en la empresa y se la realiza cada vez que se tiene algún problema, pueden ser conflictos de direcciones *IP* en la red o problemas de fugas de información. Tampoco se le ha dado la importancia necesaria para tener una persona encargada de la administración de la red y dotar a esta persona de las herramientas necesarias para que realice su trabajo.

Al no tener un Administrador de la Red ocurren caídas del sistema, o de los enlaces entre las sucursales, ocasionando pérdidas por no solucionar estos inconvenientes rápidamente, teniendo que suspender la atención a clientes.

2.1.1 REQUERIMIENTOS DE *HARDWARE*

Los requerimientos de *hardware* se enfocan a la red física, a los equipos de conectividad que deberían ser reemplazados para implementar nuevos servicios y a la seguridad de la red. Por esta razón, no se ha tomado en cuenta incrementar el número de estaciones de trabajo; pero si se ha reservado un espacio de direcciones *IP* y puertos en los equipos de conectividad, para un crecimiento futuro.

2.1.1.1 Requerimientos de Equipos de Conectividad

Tecnomega posee equipos de conectividad que no ofrecen servicios de: administración de si mismos, segmentación de la red, manejo de un esquema de seguridad, etc. Por esta razón se deberá hacer un dimensionamiento de estos equipos, determinando las características técnicas que deben cumplir.

Los equipos de conectividad necesariamente deben ser administrables capa 3, para poder implementar la segmentación por *VLANs* y manejar un esquema de seguridad. Adicionalmente, se necesitarán equipos como *firewalls* para incrementar la seguridad de la red; y se puede complementar con Sistemas de Prevención de Intrusos que detectan un ataque y toman una acción para mitigar o terminar el ataque.

Los equipos deben ser compatibles con protocolos estándares de administración de redes, para según las necesidades de la empresa escoger el *Software* de Administración de Red que más convenga y que sea compatible con los equipos existentes y los que se necesiten en el rediseño. El protocolo de administración de redes más comúnmente soportado por los equipos de conectividad es *SNMP* en sus versiones 1 y 2, sería bueno tener compatibilidad con la versión 3 para tener un nivel de seguridad mayor.

La infraestructura de telefonía de la empresa es aislada en cada sucursal, teniendo que llamar a otra sucursal por medio de la operadora Andinatel o Pacifictel según sea el caso de la ubicación de la sucursal. Por esto se quiere realizar la interconexión entre las sucursales y enlazando las centrales telefónica, para disminuir costos en las comunicaciones telefónicas.

Los equipos utilizados en el Sistema Integrado de Telefonía deben cumplir con protocolos estándar para que se puedan interconectar equipos de diferentes marcas, a la red de centrales y teléfonos.

2.1.2 REQUERIMIENTOS DE *SOFTWARE*

La plataforma utilizada en Tecnomega es íntegramente de *Microsoft*, los sistemas operativos instalados en las estaciones de trabajo son *Windows XP Profesional*, *Windows 2000 Profesional*, *Windows 98 SE*; en los servidores se tiene instalado *Windows 2000 Server* y los Sistemas de Base de Datos que se ejecutan en *SQL Server 7.0*.

En la empresa se tiene la orden de actualizar esta plataforma para que todas las estaciones de trabajo ejecuten *Windows XP Profesional* y los servidores *Windows 2003 Server*, que si bien es cierto no son los últimos sistemas operativos de *Microsoft*, pero todavía hay soporte para ellos y son más estables que las nuevas versiones de *Windows Vista Bussiness* (para estaciones de trabajo) y *Windows Server 2008* (para servidores).

La actualización de la plataforma de Sistemas Operativos es para que tengan soporte y actualizaciones por un período de 3 años para justificar la inversión en la compra de licencias. *Windows XP* tiene soporte hasta el 2010 dado que *Windows Vista* fue lanzado para Latinoamérica en febrero del 2007; *Windows 2003 Server* también tiene 3 años más de soporte porque *Windows Server 2008* todavía no ha sido liberado en su versión final.

El Sistema de Base de Datos es *SQL Server 7.0*, el cual ya no tiene soporte por parte de *Microsoft* (un producto *Microsoft* tiene soporte por tres años después del lanzamiento de una nueva versión). Sin soporte un programa, no tiene actualizaciones ni soporte técnico.

El Sistema de Base de Datos al momento se ejecuta en *SQL Server 7.0*; se tiene el proyecto de migrar a *SQL Server 2000* que ya no es la última versión pero todavía está vigente y ya se tiene compradas las licencias. Esa fue la razón que dio el Gerente de Sistemas. Sin embargo, *SQL Server 2000* quedará sin soporte cuando se lance al mercado *SQL Server 2008*.

La actualización de *SQL Server 7.0* a *SQL Server 2000* no solo es por la falta de soporte de la versión, sino que se tiene algunas mejoras en *SQL Server 2000* con respecto al anterior, que son las siguientes:

- Soporte *XML* Nativo: *XML* es un lenguaje muy utilizado, en plataformas heterogéneas. *XML* es un metalenguaje, es decir es un lenguaje de lenguajes, con el que se logra tener compatibilidad entre diferentes sistemas y lenguajes de programación
- Aumento de desempeño, disminuyendo el tiempo de respuesta en consultas, transacciones y en la administración de la base de datos
- Replicación de Bases de Datos mejorada, en *SQL Server 2000* se tienen más opciones de réplica de base de datos y es más rápida.
- La implementación de *datawarehouse* de *SQL Server 2000* tiene funciones de minería de datos (es la búsqueda de datos para identificar tendencias y establecer relaciones), que van a ser utilizadas en el desarrollo del Sistema de Información Gerencial.

La base de datos de la página *web* se ejecuta en *MySQL*, que es un Sistema de Base de Datos gratuito que está cada día mejorando y es el más utilizado en páginas *web* con bases de datos en Internet. No se adquirió el *Hosting* con servidores *Windows* por su alto costo, y adicionalmente si se va a utilizar *SQL Server* para la página *web* se tiene que pagar una licencia adicional, para que *n* clientes accedan a la base de datos.

El *Software* Empresarial que se maneja es *Global Commerce*, el cual fue comprado al desarrollador del sistema la empresa *FutureSoft S.A.* La licencia que se adquirió no solo es para su uso, ya que se compró el código fuente y el permiso para modificar el sistema para uso interno.

Teniendo en cuenta esto, la empresa no está interesada en adquirir nuevos sistemas o actualizarlos porque el *software* está hecho a la medida de sus necesidades y es modificado por el Departamento de Sistemas, cuando nace una necesidad adicional para incluir alguna nueva funcionalidad.

2.1.3 REQUERIMIENTOS DE SEGMENTACIÓN DE LA RED

La segmentación de la red es vital para incrementar el rendimiento y la seguridad. El direccionamiento *IP* está mal diseñado porque no se divide el dominio de *broadcast*, se debería segmentar la red en subredes para cada sucursal no se ha hecho esto por no incorporar equipos costosos que interconecten las redes de las sucursales, como son los ruteadores.

El rendimiento de la red decae drásticamente por tormentas de *broadcast* ocasionadas por tener un dominio de colisión grande, de más de 80 computadores conectados a la red de Quito en una sola red clase B. El momento que un computador esté infectado con un virus que arroja basura a la red para colapsarla, esto ocasiona pérdidas porque se interrumpe las actividades de la empresa.

Dado el bajo rendimiento de la red por la inclusión de *hubs* y por la falta de administración de la misma, se tuvieron que contratar enlaces de *Internet* para cada una de las sucursales porque cuando se tenía una sola conexión centralizada, se compartía esta por medio de los enlaces entre las sucursales y el servicio era demasiado lento, por el colapso de la red.

Para la segmentación de la red se diseñará el direccionamiento *IP* y se dimensionarán los equipos de conectividad que interconecten las redes de las diferentes sucursales. Se debe tener por lo menos una red por cada sucursal, para no tener dominios de colisión muy grandes y mejorar el rendimiento.

Adicionalmente, se debe reservar una capacidad de crecimiento para las subredes que se asignen a las sucursales y otras subredes para nuevas sucursales o nuevos servicios.

2.1.4 ANÁLISIS DE REQUERIMIENTOS SEGURIDAD EN LA RED

La seguridad de la información es muy importante en la actualidad, para esto se debe crear una política de seguridad, que establezca lo que se quiere proteger, cómo se lo va a proteger y las medidas de seguridad que se deben tomar para proteger la información. Hecho esto se tendrá una idea de los equipos que se necesitan para cumplir con las expectativas de seguridad de la empresa.

La principal información que se desea proteger es la almacenada en los servidores de la empresa que contienen importantes bases de datos de: clientes, *stock*, cuentas por cobrar, cuentas por pagar, etc. Esta información es muy importante para la empresa.

La seguridad que se implemente debe cumplir: autenticación, autorización y contabilidad; no se puede permitir el ingreso de usuarios no autorizados. Los usuarios deben autenticarse y solo así podrán ingresar a la red; además se debe llevar registros de lo que hizo cada usuario en el sistema. De esta manera se logrará así una seguridad estricta, para salvaguardar la información organizacional.

Otro punto débil, es la interconexión de las sucursales y la réplica de información para actualizar los productos y el *stock* en la página *web*, que realiza la transferencia de información en texto plano, las que podrían ser víctimas de un espía que robe la información o la cambie. Para eliminar esta vulnerabilidad se tiene pensado el uso de *VPN* para la conexión entre sucursales y las transferencias de información que se envíen por *Internet*.

La importancia del manejo de contraseñas es crucial, este tema debe ser tratado dentro de las políticas de seguridad, se debe tener una política que obligue a los usuarios de la red a cambiar las claves de sus computadores periódicamente, aun más en servidores y equipos de conectividad.

Adicionalmente las claves son débiles porque no incorporan caracteres alfanuméricos combinados con caracteres especiales; deben tener una longitud mínima de 8 caracteres y sería recomendable contraseñas de más de 8 caracteres porque es más difícil que se quiera romper la clave usando el método de fuerza bruta.

2.2 ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS PARA EL REDISEÑO DE LA RED

2.2.1 TECNOLOGÍAS PARA REDES LAN

Las tecnologías más utilizadas en la actualidad para redes LAN son: *Fast Ethernet* (100 Base - TX) y *Gigabit Ethernet* (1000 Base - T), por su facilidad de instalación, mantenimiento y por sus bajos costos de equipos compatibles. En las siguientes secciones se profundizará en estas dos tecnologías.

2.2.1.1 *Fast Ethernet*^{4/5}

Fast Ethernet es la evolución de *Ethernet*, en la que se mejoró las velocidades existentes manteniendo el mismo protocolo. *Ethernet* inventada en 1973 por *Digital, Intel y Xerox*, es la tecnología de redes LAN más utilizada en el mundo.

Esta tecnología de medios compartidos está basada en tramas, que se envían a todos los nodos de la red, pero solo el nodo destino del mensaje puede leerlo, ya que en la cabecera de la trama se especifica el destinatario; si un nodo no es el destinatario lee el encabezado y desecha la trama.

⁴ <http://es.wikipedia.org/wiki/Ethernet>

⁵ http://es.wikipedia.org/wiki/Fast_Ethernet

Ethernet puede ser implementada con cable coaxial, par trenzado o fibra óptica. Pero el más comúnmente utilizado es el par trenzado, gracias a su facilidad de instalación y mantenimiento. Hoy en día, ya no son muy comunes las redes con cable coaxial; las redes de fibra óptica son más utilizadas cuando la distancia que se necesita no se puede alcanzar con par trenzado o para redes de más alta velocidad, como por ejemplo 10 *Gigabit Ethernet*.

Dada la necesidad de mayores velocidades en las redes nació la idea de mejorar el estándar *Ethernet*, porque se necesitaba ejecutar aplicaciones con interfaces gráficas y manejar mucha más información que saturaba la capacidad de transmisión de las redes existentes.

Entonces *IEEE* convocó al grupo de 802.3 para que creara una *Ethernet* más rápida en 1992, con dos objetivos específicos:

- Mantener 802.3 como estaba, pero aumentar su velocidad.
- Rehacer el estándar totalmente para darle características nuevas, como: tráfico en tiempo real, voz digitalizada y mantener el mismo nombre de 802.3 por mercadeo.

El grupo 802.3 escogió mantener *Ethernet* como estaba e incrementar la velocidad por las siguientes razones:

- De ser el nuevo estándar debe ser compatible con las redes existentes
- Siguiendo con el mismo protocolo *Ethernet*, no se van a tener los problemas de un protocolo nuevo e inestable.
- Rápido desarrollo del estándar antes de que la tecnología cambie.

El nombre del estándar *Ethernet* mejorado es 802.3u (*Fast Ethernet*), que fue aprobado en junio de 1995 por la *IEEE*. 802.3u no es un nuevo estándar sino una modificación al estándar 802.3. La idea principal de *Fast Ethernet* era mantener los formatos anteriores, las interfaces, los procedimientos y reducir el tiempo de bit a 10 ns de 100 ns que establece el estándar *Ethernet*.

Los cables que soportan *Fast Ethernet*; son:

- Cable *UTP* categoría 3 era el más utilizado por compatibilidad con redes existentes en esa época, se lo tomó en cuenta a pesar no poder llevar la señal a 100 *Mbps* con codificación *Manchester* a 100 metros.
- Cable *UTP* categoría 5 cumple con todos los requerimientos de velocidad de transmisión y esquemas de codificación de 802.3u
- Cable de Fibra Óptica cumple con todos los requerimientos de velocidad de transmisión y esquemas de codificación de 802.3u

Nombre	Cable	Longitud máxima	Modo	Codificación
100 Base – T4	<i>UTP</i> categoría 3	100 metros	<i>Half dúplex</i>	8B / 6T
100 Base - TX	<i>UTP</i> categoría 5	100 metros	<i>Half dúplex</i>	4B / 5B
100 Base - FX	Fibra Óptica	2000 m	<i>Full dúplex</i>	NRZI

Tabla 2-1: Estándares *Fast Ethernet*^{6,7}

En *Fast Ethernet* se aplican todas las reglas del estándar *Ethernet*, por ejemplo el algoritmo de retroceso exponencial binario y una sola estación puede transmitir a la vez, etc., por lo que funciona como el antiguo *Ethernet*.

2.2.1.2 *Gigabit Ethernet*⁸

Muy poco después de la estandarización de *Fast Ethernet* el grupo 802.3 empezó a trabajar en una versión más rápida, conocida como *Gigabit Ethernet*. *IEEE* aprobó *Gigabit Ethernet* bajo el nombre 802.3z en 1998; su objetivo principal era al igual que 802.3u aumentar la velocidad de su antecesor en 10 veces y mantener la compatibilidad hacia atrás.

Todos los enlaces de *Gigabit Ethernet* son punto a punto a diferencia de los múltiples tipos de enlaces que se utilizan en *Ethernet*. *Gigabit Ethernet* soporta dos modos de transmisión: *full* dúplex y semidúplex.

⁶ <http://es.wikipedia.org/wiki/100Base-TX>

⁷ http://www.consulintel.es/html/Tutoriales/Articulos/fast_eth.html

⁸ http://en.wikipedia.org/wiki/Gigabit_Ethernet

El modo predefinido es el *full* dúplex, donde el tráfico fluye en ambas direcciones al mismo tiempo. Este modo funciona cuando los computadores están conectados a un conmutador o más. Para que el computador pueda enviar tramas en cualquier momento se tiene un búfer, por lo que el conmutador puede variar o igualar la velocidad.

El segundo modo es semidúplex que funciona cuando las computadoras están conectadas a un concentrador en vez de un conmutador. Los concentradores no almacenan en un búfer las tramas entrantes, solo conectan las estaciones como que estuvieran conectadas a un mismo cable con múltiples derivaciones. Por esto se pueden producir colisiones y se utiliza CSMA/CD estándar.

Gigabit Ethernet es cien veces más rápida que *Ethernet*, por lo que la distancia debe ser cien veces menor (25 metros) por las colisiones. 25 metros es una distancia demasiado corta para una red por lo que se hace una extensión de portadora para incrementar el tiempo de transmisión y poder manejar más fácilmente las colisiones. La extensión de portadora se realiza en el *hardware* del emisor y cuando llega al receptor se la elimina, lo que aumenta la velocidad del mismo.

Gigabit Ethernet utiliza una tecnología de envío de ráfagas de tramas para optimizar el uso del canal, con la extensión de portadora se disminuye la eficiencia del esquema. Las ráfagas de tramas aprovechan la acumulación de tramas para mandarlas en ráfagas concatenadas optimizando el canal.

Nombre	Cable	Segmento Máximo	Codificación
1000 Base – SX	Fibra Óptica	550 m	8B / 10B
1000 Base – LX	Fibra Óptica	5000 m	8B / 10B
1000 Base – CX	2 pares STP	25 m	8B / 10B
1000 Base – T	4 pares UTP	100 m	4D-PAM5

Tabla 2-2: Estándares *Gigabit Ethernet*

2.2.2 TECNOLOGÍAS PARA REDES WAN Y REDES DE ACCESO

Los servicios WAN y las redes de acceso disponibles en Ecuador, son los siguientes:

- *ADSL*
- *Metro Ethernet*
- *ATM*
- *WIMAX*

2.2.2.1 Línea Digital Asimétrica de Suscriptor (*ADSL*)

Consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional. En el Servicio de *Internet* por *modem* telefónico se manejan velocidades bajas porque las líneas telefónicas fueron creadas para transportar señales de voz, limitando el ancho de banda en las centrales telefónicas al del tráfico de voz.

La limitación del ancho de banda se realiza con un filtro que atenúa las frecuencias por debajo de 300 *Hz* y por arriba de 3400 *Hz*; estas frecuencias son los puntos de media potencia (-3 *dB*), la distancia entre los puntos de media potencia es de 3100 *Hz*. Este ancho de banda no es suficiente para las necesidades de transferencia de datos de hoy en día, peor aún telefonía y videoconferencia *IP*.

Teniendo en cuenta las necesidades de mayor capacidad en los canales de acceso a *Internet* se creó *ADSL*. Esta tecnología utiliza la capacidad restante de los cables de cobre de las líneas telefónicas para conectarse a un conmutador diferente, que no tiene el filtro para limitar el ancho de banda al de la voz, logrando tener todo el ancho de banda del circuito local. La capacidad del circuito local se ve limitada por varios factores: longitud de la central al abonado, espesor del cable de cobre y calidad del mismo.

Los objetivos principales del *ADSL* son:

- *ADSL* debe funcionar sobre los circuitos locales existentes de par trenzado categoría 3.
- *ADSL* no debe afectar el funcionamiento de máquinas de fax, ni teléfonos existentes.
- *ADSL* debe superar la velocidad de 56 *Kbps*.

Se tienen dos opciones alternativas de implementación para *ADSL*.

- La primera de *AT&T* funciona dividiendo las frecuencias del circuito local de 1.1 *MHz* en tres bandas: una para el servicio telefónico, otra para el canal ascendente y una tercera el canal descendente.
- La segunda, Multitono Discreto (*DMT*), divide el espectro de 1.1 *MHz* en 256 canales independientes de 4312.5 *Hz* cada uno. El canal 0 se utiliza para el servicio telefónico, los canales del 1 al 5 no son utilizados para evitar interferencia. Los 250 canales restantes se dividen así: uno para control de flujo ascendente, otro para el control de flujo descendente y el resto para datos del usuario.

Esta tecnología se la llama asimétrica porque del 80 al 90 % del canal se la dedica a la capacidad descendente y de un 10 a 20 % a la capacidad ascendente. Hablando de canales se suele utilizar 32 canales para el flujo ascendente y los restantes para el descendente. La mayoría de usuarios utiliza el *Internet* para descargar archivos, información, etc.; por lo que se necesita una capacidad mayor de descarga y una menor para enviar información hacia el *Internet*.

En el mercado ecuatoriano no se ofrecen estas velocidades ni en los planes más altos corporativos, lo máximo que se tiene disponible es de 2 *Mbps* X 512 *Kbps* a \$ 759 dólares mensuales; este servicio lo brinda *Interactive*⁹.

⁹ Precio obtenido de www.interactive.net.ec, en la sección de productos.

En este tipo de servicio la calidad de la línea telefónica es muy importante y se ajusta automáticamente la capacidad de transmisión. La relación señal a ruido nunca es relativamente buena para tener velocidades ideales de más de 11 *Mbps*; la velocidad más alta que se puede llegar es de 8 *Mbps*.

El esquema que se maneja en *ADSL* es instalar un Dispositivo de Interfaz de Red (*NID*) en el lado del usuario para acceder al servicio, éste es el límite entre la propiedad de la compañía telefónica y la propiedad del usuario. Junto al modem *ADSL* se suele instalar un filtro para dividir la señal de datos con la de voz. La mayoría de módems *ADSL* son externos y se conectan al computador del cliente por medio de redes *Ethernet* o cable *USB*.

En el otro extremo está el proveedor del servicio, el cual tiene instalado un divisor correspondiente para que separe las señales de voz de las de datos; las de voz se envían al conmutador de voz normal y las de datos se envían al Multiplexor de Acceso a Línea Digital de Suscriptor (*DSLAM*), en el que luego de ser procesadas las señales se envían al *ISP*.

ADSL tiene una versión con características inferiores para disminuir costos de equipos e instalación en el lado del cliente, esta tecnología se llama *G.lite*. La diferencia principal es que no se tiene que instalar un divisor de frecuencias en el lado del cliente sino que se instala micro filtros en cada teléfono o fax y en el modem *ADSL*; estos filtros para los teléfonos atenúan frecuencias mayores a 3400 *Hz* y el del módem las frecuencias mayores a 26 *KHz*. Esto hace que la velocidad máxima disminuya a 1.5 *Mbps* de 8 *Mbps*.

2.2.2.2 Metro Ethernet

La Red *Metro Ethernet* es una arquitectura de red destinada a brindar servicios de conectividad para redes *MAN/WAN* de nivel 2, a través de interfaces *Ethernet*. Estas redes multiservicio soportan aplicaciones y sistemas de tiempo real, *streaming*, flujo de datos de audio y/o video.

Los beneficios que *Metro Ethernet* ofrece son:

- Fácil uso: tener una sola tecnología de redes *LAN* y *WAN* facilita la operación de la red, administración, manejo y actualización
- Economía: la interconexión con tecnología *Metro Ethernet* se caracteriza por:
 - Amplio uso: se emplean interfaces *Ethernet* que son las más utilizadas en redes.
 - Bajo costo: ofrece un bajo costo en la administración, operación y funcionamiento de la red.
 - Capacidad de Transmisión: permite a los usuarios acceder a conexiones de banda ancha a menor costo.
- Flexibilidad: permite modificar y manipular de una manera más dinámica, versátil y eficiente, la capacidad de transmisión y la cantidad de usuarios en corto tiempo.

Metro Ethernet tiene una arquitectura compuesta por una red conmutada *MEN (Metro Ethernet Network)*, que la ofrecen a través del proveedor de servicios de telecomunicaciones. Los usuarios acceden a la red mediante equipos, tales como: routers, conmutadores que se conectan a través de *UNIs (User Network Interface)* a velocidades de 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps.

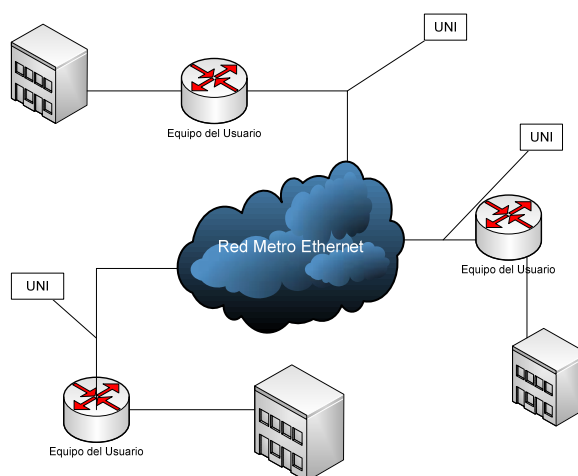


Figura 2-1: Arquitectura *Metro Ethernet*

2.2.2.2.1 Conexiones Virtuales Metro Ethernet

Una Conexión Virtual *Metro Ethernet* (EVC) es la asociación de dos o más *UNIs*, y tiene las siguientes funciones:

- Conectar dos o más sitios para transferir tramas *Ethernet* entre ellos.
- Impedir la transferencia de tramas entre diferentes clientes que forman un EVC, incrementando la seguridad y la privacidad de cada cliente.

Los EVC son frecuentemente utilizados para levantar *VPNs* de nivel 2. El Foro *Metro Ethernet* ha definido dos clases de EVC, que son las siguientes:

- *E – Line*, para enlaces punto a punto. Provee un servicio simétrico bidireccional para enviar datos. En este servicio especifica una Velocidad de Información Comprometida (*CIR*), un Tamaño Comprometido de la Trama (*CBS*), una Velocidad de Información en Exceso (*EIR*) y un Tamaño de la Trama en Exceso (*EBS*), que dependen de cada proveedor de servicio de telecomunicaciones. Normalmente los *E – Line* son utilizados para acceso a *Internet*.
- *E – LAN*, para enlaces multipunto a multipunto, conectando dos o más *UNIs*. El cliente envía datos y los puede recibir en una o más *UNIs*, en cada una de las sucursales está instalada una *UNI* conectada a un EVC multipunto; si se desea agregar una sucursal se conectan al mismo EVC multipunto, simplificando la instalación y la configuración.

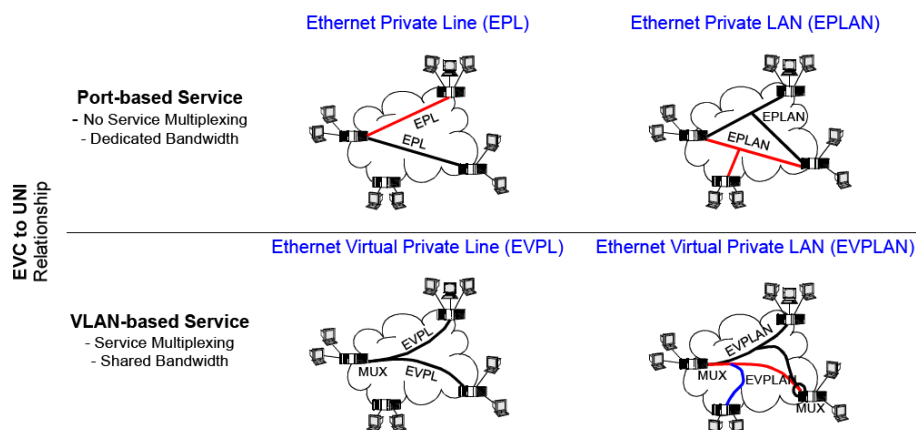


Figura 2-2: Conexiones Virtuales *Metro Ethernet*¹⁰

¹⁰ Grafico obtenido de *Trend's Metro Ethernet* Guía de Bolsillo

2.2.2.2.2 Clases de Servicio en Metro Ethernet

Metro Ethernet ofrece tres clases de servicio que son:

- Puerto Físico, que da el servicio a un usuario; todo el tráfico que entra o sale del puerto recibe la misma clase de servicio.
- *CE-VLAN* Clase de Servicio (802.1p), utiliza etiquetas para diferenciar las clases de servicio, se pueden tener hasta 8 clases de servicio.
- Diferenciación de Servicio / Tipo de Servicio *IP*, si se utiliza *IP ToS* se puede tener 8 clases de servicio conocidas como Prioridad *IP*. Cuando se utiliza Diferenciación de Servicio se define como Comportamiento por Salto (*PHS*), con esto se obtienen hasta 64 clases de servicio.

2.2.2.2.3 Soporte de Etiquetas para VLANs

Las *VLANs* pueden utilizarse para segmentar la red o para interconectar redes; por lo general los equipos de conectividad, como conmutadores o ruteadores pueden leer etiquetas para establecer clases de servicio o prioridades y los computadores no. Por esto se tiene tramas etiquetadas y tramas no etiquetadas.

2.2.2.2.4 Aplicaciones de Metro Ethernet

Acceso dedicado a Internet

Los usuarios corporativos buscan altas velocidades para acceder a Internet por el alto número de empleados que tiene su empresa, *Metro Ethernet* es una buena opción por las velocidades que maneja esta tecnología. Un *EVC* puede solucionar el acceso del usuario al Proveedor de Servicio de *Internet (ISP)*.

Extensión de Redes LAN

Las empresas con múltiples sucursales que tienen redes LAN en cada una de ellas buscan soluciones que integren sus redes LAN. Estas sucursales se pueden interconectar a altas velocidades como si estuvieran en la misma LAN, gracias a las redes *Metro Ethernet*. La conexión entre dos sucursales se puede realizar por medio de *E – Line* o *E – LAN*; si se tiene más de dos sucursales se deben utilizar *E – LAN*, creando las VLANs necesarias.

Intranet / Extranet Nivel 2 VPN

Metro Ethernet es una buena alternativa para conectar la *Intranet* de una empresa con sitios remotos o conexiones *Extranet*. Las conexiones *Extranet* normalmente son para que los socios de negocios o clientes accedan a cierta parte permitida de la red de la empresa, desde sus oficinas o domicilios.

2.2.2.3 Modo de Transferencia Asíncrona (ATM)

En los años 60 se tuvo la primera referencia de *ATM* cuando un norteamericano de los Laboratorios *Bell* describió y patentó un modo de transferencia no síncrono. El *CCITT* en 1988 decidió que *ATM* sería la nueva tecnología para redes de banda ancha. Se desechó la idea de la transmisión síncrona y se empezó a discutir el tamaño de las celdas.

Los representantes de Estados Unidos proponían celdas de 64 *bytes* y los representantes de Europa pensaron en celdas de 32 *bytes*, los europeos decían que las celdas grandes de 64 *bytes* involucrarían retardos inaceptables, que no permitiría transmitir voz de buena calidad obligando a instalar canceladores de eco. Luego de muchas discusiones y ningún acuerdo se tomó una decisión, las celdas se fijaron en 48 *bytes* de datos y 5 *bytes* de cabecera sumando un total de 53 *bytes*.

2.2.2.3.1 Circuitos Virtuales en ATM

Las redes *ATM* son orientadas a conexión, para establecer la conexión se requiere que se envíe un paquete de establecimiento de la conexión que a medida que va pasando entre los conmutadores van creando entradas en sus tablas internas de la existencia de la conexión y reservando recursos para la conexión.

Estas conexiones son llamadas circuitos virtuales; la mayoría de redes *ATM* soportan circuitos virtuales permanentes que son conexiones permanentes entre dos *host*. Cada una de estas conexiones tiene un identificador de conexión único, este identificador es almacenado en la cabecera de la celda para que el *host* origen, destino y los conmutadores intermedios sepan a qué conexión pertenece la celda, facilitando el envío correcto de las mismas.

La razón para tener celdas pequeñas de tamaño fijo es porque la conmutación de celdas se hace por *hardware* y así se facilita la construcción de estos equipos, y se bajan los costos. Por ejemplo, en el envío de paquetes *IP* de longitud variable se hace el enrutamiento mediante *software* y se demora más tiempo su envío. Las celdas de longitud pequeña no bloquean los canales de transmisión, por lo que se facilita la implementación de QoS.

Otra ventaja de *ATM* es la facilidad para *multicast*, el *hardware* se puede configurar para enviar una celda entrante a varias salidas, procedimiento necesario para transmitir programas de televisión a varios receptores.

La entrega de las celdas en *ATM* no es garantizada pero el orden de las mismas si lo es. Las celdas se pueden perder en el trayecto, pero *ATM* no se encarga de retransmitir estas celdas sino que la recuperación de las celdas les corresponde a los niveles más altos de los protocolos.

ATM trabaja a diferentes velocidades de transmisión, así velocidades de: 155 *Mbps* y 600 *Mbps* son las más comunes; existen velocidades superiores pero no están disponibles en el Ecuador. Con 155 *Mbps* se puede transmitir televisión de alta definición por eso fue escogida esta velocidad y adicionalmente es compatible con *SONET* de *AT&T*.

2.2.2.3.2 Modelo de Referencia ATM

Este modelo es diferente al modelo *OSI* y al *TCP/IP*, se define como si fuera tridimensional. Entonces se habla de planos: de administración de capas, de usuario y de control; a continuación se especifican las capas del modelo:

- Capa Física, se encarga de la especificación de voltajes, temporizadores de *bits*, etc. Además se especifica que las celdas *ATM* se deben mandar sin modificaciones por cable o fibra óptica, pero también se pueden empaquetar dentro de la carga útil de otros sistemas de transporte, garantizando la independencia del medio de transmisión.

Esta capa se divide en dos subcapas:

- Subcapa Dependiente del medio: se ocupa de interactuar con el medio de transmisión real, la capa es diferente para transportadoras y para cables.
- Subcapa de Convergencia de Transmisión: esta capa recibe celdas y envía una cadena de *bits* a la capa inferior tomando en cuenta cuando inicia y termina una celda para que en el otro lado se puede reensamblar la celda.
- Capa *ATM*, se encarga de las celdas y su transporte. Se define la estructura de la celda y se indican sus campos. También se especifica el establecimiento, liberación de los circuitos virtuales y el control de congestión.
- Capa de adaptación *ATM*, esta capa se encarga de segmentar los paquetes que son más grandes que la celda, los transmite

individualmente y en otro extremo los reensambla. Esta capa se divide en dos subcapas:

- Subcapa de Segmentación y Reensamblaje: esta subcapa se encarga de fragmentar los datos en celdas en el lado de transmisión y en el lado de recepción hace el proceso inverso; esto es, une las celdas para recuperar los datos segmentados.
- Subcapa de Convergencia: permite la diferenciación de los servicios para que se puedan transportar en la red *ATM* según la clase de servicio que necesita los datos.

El plano de usuario se encarga del transporte de los datos, el control de flujo, la corrección de errores y otras funciones de usuario. El plano de control se encarga de administrar la conexión entre los dos computadores que están transmitiendo información.

ATM es muy utilizado en el sistema telefónico, para transportar paquetes *IP* internamente; los usuarios no se percatan que el proveedor tiene infraestructura *ATM* porque se accede a esta red mediante la tecnología *ADSL*, pero esta tecnología está en uso y seguirá estando.

2.2.2.4 IP MPLS

Multiprocol Label Switching (MPLS) es un estándar para el transporte de datos desarrollado por la *IETF* y definido en la *RFC 3031*. *MPLS* opera entre las capas: enlace de datos y red del modelo *OSI*. Está diseñado para unificar el transporte de datos para redes basadas en circuitos y paquetes. Puede transportar diferentes tipos de tráfico, como: paquetes *IP*, *VoIP*, etc.

MPLS es una tecnología de conmutación que proporciona circuitos virtuales en redes *IP*, anexando un encabezado a cada paquete *IP*. El encabezado contiene una o más etiquetas de cuatro campos cada una.

Los paquetes *MPLS* son enrutados por sus etiquetas mas no por su dirección *IP*, este ruteo por etiquetas es más rápido que el ruteo *IP*. *MPLS* es independiente del transporte de la capa de enlace de datos del modelo *OSI*.

Los ruteadores de entrada son llamados *Label Edge Router (LER)*, estos ruteadores enlazan la red *MPLS* y otras redes. Los ruteadores que realizan la conmutación de etiquetas son los *Label Switching Router (LSR)*. Un *LER* es un *LSR* que puede enrutar los paquetes a otras redes diferentes a *MPLS*.

Las etiquetas son distribuidas utilizando *Label Distribution Protocol (LDP)*; mediante este protocolo los ruteadores intercambian información de la red para alcanzar otros ruteadores. Esto es parecido a los protocolos que consolidan las tablas de enrutamiento en los ruteadores.

En *MPLS* se puede establecer rutas mediante *Label Switched Path (LSP)*, que son muy útiles para establecer una *VPN*. Cuando un paquete no etiquetado accede a un ruteador de ingreso y requiere pasar a través de un túnel *MPLS*, el ruteador tiene que determinar la *Forwarding Equivalence Class (FEC)* para luego insertar una o más etiquetas *MPLS*.

2.2.2.4.1 Arquitectura *MPLS*

La arquitectura de las redes *MPLS* está compuesta por:

- *LER*: es el equipo que inicia o termina el túnel *MPLS* (pone o quita etiquetas); existen ruteadores de entrada o salida, llamados *LER*, porque se encuentran en los extremos de la red *MPLS*.
- *LSR*: equipo de que conmuta etiquetas.
- *LSP*: es el nombre de la ruta, es decir, del túnel *MPLS* establecido entre los extremos. Los *LSP* son unidireccionales.
- *LDP*: es un protocolo de distribución de etiquetas *MPLS*.
- *FEC*: categoriza el tráfico encaminado por una etiqueta.

2.2.2.4.2 Cabecera MPLS



Figura 2-3: Cabecera MPLS

Donde:

- *Label* (20 bits): es la identificación de la etiqueta.
- *Exp* (3 bits): está reservado para bits experimentales.
- *S* (1 bit): *stack* este bit indica cuando se tiene etiquetas apiladas o en *stack*, S=0 indica que existen más etiquetas apiladas, S=1 es la última etiqueta del *stack*.
- *TTL* (8 bits): tiene la misma funcionalidad que en el protocolo *IP*, decrementa su valor cada que pasa por un ruteador y cuando llega a 0, el paquete es descartado.

2.2.2.5 WIMAX

WIMAX son las siglas de “*Worldwide Interoperability for Microwave Access*” y funciona bajo el estándar de la *IEEE 802.16*. Este estándar permite conexiones similares a *ADSL* o a *CABLE MODEM*, sin cables y a distancias de 50 a 60 Km y es compatible con estándares como *Wi-Fi* (802.11).

WIMAX será la red metropolitana más importante para acceso a *Internet* y tendrá alcance para zonas que antes no tenían servicio de *Internet* de Banda Ancha por medio de *ADSL* o *CABLE MODEM*. Las empresas pueden utilizar *WIMAX* para sus comunicaciones internas, para implementar *Intranets* o *Extranets*. *WIMAX* también impulsará el desarrollo en Ecuador de *VoIP* con teléfonos inalámbricos o celulares con capacidades *Wi-Fi*.

2.2.2.5.1 Características de WIMAX

WIMAX tiene características muy favorables para su uso, es una tecnología pensada para ser una solución integral de última milla para usuarios fijos y móviles, por esto existen algunos estándares dentro de 802.16.

A continuación se citan algunas características:

- Altas velocidades a más larga distancia.
- Calidad de Servicio
- Compatibilidad entre fabricantes, se pueden adquirir equipos de más de un fabricante e instalarlos en un mismo sistema.
- Es un sistema escalable:
 - Brinda fácil adición para aumentar la capacidad de las celdas.
 - Se permite usar bandas licenciadas como no licenciadas para aumentar la capacidad del sistema
- Cobertura
 - Modulación adaptiva para disminuir la velocidad de transmisión para tener mayor rango de cobertura.

2.2.2.5.2 Modelos de WIMAX

a) Modelo Fijo

El estándar *IEEE* 802.16 fue diseñado para brindar un acceso a la red WIMAX para clientes fijos o estáticos inalámbricamente. Para tener este servicio se debe instalar una antena en el domicilio u oficina del cliente; usualmente la antena se instala en un mástil en el exterior del edificio o casa para tener una mejor señal. WIMAX también puede ser utilizado en interiores por lo que necesita ser tan robusto como para exteriores.

WIMAX de acceso fijo funciona en las bandas: 2.5 GHz en banda licenciada, en 3.5 GHz y 5.8 GHz en banda libre (sin licencia). Esta tecnología es una competencia para *CABLE MODEM* y *ADSL*. *WIMAX* es buena alternativa ya que no necesita mayor infraestructura instalada en el domicilio u oficina del cliente, adicionalmente no necesita la calidad de la línea telefónica ni de distancias a la central telefónica para limitar la velocidad de acceso.

b) *Modelo Móvil*

El estándar 802.16e está dedicado al mercado móvil, usa la tecnología de Acceso Múltiple por División Ortogonal de Frecuencia (*OFDMA*); al igual que *OFDM* se divide en subportadoras y éstas se agrupan formando subcanales. Se tienen dos opciones: un solo usuario utiliza todos los subcanales en un determinado instante teniendo mayor velocidad, o múltiples clientes puedan transmitir información utilizando unos o más subcanales del total disponible.

Se ha logrado mejorar la tecnología de 802.16 para mitigar los problemas de:

- Interferencia Multicamino
- Retraso Difundido
- Robustez

Los dos primeros ítems mejoran la conectividad de la estación del usuario a la estación base del servicio cuando no existe línea de vista. También se ha desarrollado una tecnología para Control de Acceso a Medios Emergentes en el estándar para enlaces de gran distancia donde se pueden tolerar retrasos.

Cuando *WIMAX* trabaja en bandas no licenciadas utiliza Duplicación por división de tiempo (*TTD*) y cuando trabaja en bandas licenciadas utiliza *TTD* o Duplicación por división de frecuencia (*FDD*). El estándar 802.16 usa *OFDM* para la optimización de servicios inalámbricos de datos; *OFDM* divide a su portadora en 256 subportadoras en lugar de 64 como en 802.11, al tener más subportadoras en la misma banda se tiene portadoras más estrechas.

Con 256 subportadoras se puede tener una cobertura en un área de 48 Km, con conexiones de estaciones de usuario sin línea de vista a una velocidad de hasta 75 *Mbps* con una eficiencia espectral de 5 *bps/Hz*, pudiendo dar soporte a miles de usuarios y pudiendo incrementar la capacidad de transmisión de los canales. Adicionalmente, *WIMAX* soporta Acuerdos de Nivel de Servicio (*SLA*), y Calidad de Servicio.

2.2.2.5.3 *WIMAX en Ecuador*

a) ***Proyecto de WIMAX en las Islas Galápagos realizado por Intel***¹¹

En Ecuador se tiene un proyecto de *Intel* para implementar *WIMAX* en la Estación Científica Charles Darwin en Galápagos, donde se quiere interconectar las islas del Archipiélago de Galápagos para probar la tecnología con largas distancias que separan las islas y también por las condiciones físicas y meteorológicas. Esta implementación deberá ser realizada sin que los equipos instalados interfieran con el ecosistema de las Islas y bajo la legislación de telecomunicaciones del Ecuador.

b) ***Grupo TV Cable instala Red WIMAX en Guayaquil***¹²

El Grupo *TV Cable* ha invertido medio millón de dólares en la implementación de una Red *WIMAX* en Guayaquil, la cual ofrece servicios de *Internet* y Telefonía. Esta tecnología está disponible para tres segmentos de mercado: usuarios residenciales, comerciales e industriales.

¹¹ Obtenido de Noticias *Intel* 2006

¹² Noticia obtenida del Diario "El Comercio"

Este nuevo servicio ofrece altas velocidades de transferencia de información y conectividad de última milla para acceso a *Internet*. Las ventajas para los usuarios son muchas, ya que no tienen que conectarse por medio de cables que se conectan a los cajetines de los proveedores de última milla instalados en los postes. Se tiene independencia de las instalaciones de cableado de los proveedores de *Internet* o las distancias a las centrales telefónicas del proveedor de telefonía, como es el caso de acceso *ADSL*.

TVCable tiene instalados tres transmisores en Guayaquil, con el cual se tiene una señal nítida en una cobertura de más de 15 Km desde la antena. Para acceder al servicio los clientes deben contar con equipos compatibles que incorporen antenas especiales y estén instalados en el exterior del lugar. Dos de los tres transmisores se han instalado en la vía a Daule, lo que evidencia la intención de entrar con esta tecnología en el sector comercial e industrial de Guayaquil.

2.2.3 TECNOLOGÍAS PARA REDES *WLAN*¹³

Las necesidades de movilidad de los usuarios de equipos de computación es muy importante hoy en día, razón por la cual *Ethernet*, que ha sido la tecnología más ampliamente usada, tiene un competidor muy fuerte, las Redes Inalámbricas de Área Local (*WLAN*). Las *WLAN* se están utilizando cada vez más en edificios de oficinas, aeropuertos, centros comerciales, restaurantes, hoteles, entre otros lugares públicos.

Las *WLAN* son muy versátiles en las oficinas, ya que son un complemento a la infraestructura cableada, brindando a los usuarios móviles una conectividad permanente. Adicionalmente permite que visitantes se conecten al Internet o a la red sin tener que conectarse físicamente, lo que implica tener puertos disponibles en el lugar donde se requiera ubicar el computador.

¹³ Material de Soporte *WLAN* Ing. Soraya Sinche

En Tecnomega se tienen algunas reuniones o eventos donde los visitantes van con sus computadores portátiles, *PDA*s, etc., para estar en contacto con sus empleados y clientes por medio de *email*, mensajería instantánea. Implementando redes inalámbricas se tendrían más visitas de los clientes y socios de negocios de la empresa, porque no se desconectarían de su oficina y pueden pasar más tiempo en las Agencias de Tecnomega.

2.2.3.1 Estándar *IEEE* 802.11

IEEE 802.11 o *Wi-Fi* es un estándar de comunicaciones que define el uso de los dos niveles más bajos de la arquitectura *OSI* (capa física y capa de enlace de datos), este estándar norma el funcionamiento en una *WLAN*.

El protocolo 802.11 estandarizado en 1997 describe tres técnicas de transmisión de la capa física: la primera el método de infrarrojos que es la misma tecnología que se usa en los controles remotos de televisión; los otros dos métodos utilizan la técnica de radio de espectro expandido, como son *FHSS* y *DSSS*. Estas dos últimas técnicas utilizan la frecuencia sin licenciamiento de 2.4 *GHz*, y una velocidad de 1 *Mbps* y 2 *Mbps*.

Al trabajar en la banda *ISM* de 2.4 *GHz* se tiene mucha interferencia con artefactos eléctricos como: puertas automáticas de garajes controladas por radio, los hornos microondas, los teléfonos inalámbricos, etc. La interferencia disminuye la velocidad efectiva al producirse muchos errores en la transmisión, debiéndose retransmitir las tramas erróneas.

En 1999 se introdujeron dos técnicas adicionales de modulación para alcanzar mayor capacidad de transmisión, éstas son Multiplexación por División Ortogonal de Frecuencia (*OFDM*) y Secuencia Directa en Espectro Extendido de Alta Velocidad (*HRDSSS*) que permiten velocidades de hasta 54 *Mbps* y 11 *Mbps*, respectivamente. En el año 2001 se introdujo *OFDM* para la frecuencia de 2.4 *GHz*, ya que la primera trabajaba en 5 *GHz*.

2.2.3.2 Redes Inalámbricas de Área Local IEEE 802.11a

El protocolo 802.11a fue estandarizado en 1999, el mismo que trabaja en la banda *C-ISM* en 5.8 GHz y opera a una velocidad máxima de 54 Mbps; la velocidad real está por los 23 Mbps. Opera desde los 5.725 GHz hasta los 5.875 GHz en la banda C no licenciada; al operar en esta banda de frecuencia las ondas son mucho más pequeñas por lo que la cobertura es menor que 802.11b/g, teniendo que instalar más equipos 802.11a para cubrir la misma área que con equipos 802.11b/g.

Usa el esquema de modulación *OFDM* en vez de *DSSS*, el cual es transmitido en 52 subportadoras en paralelo lo que da mayor resistencia a interferencia y mejor velocidad. Esta tecnología con mayor velocidad da la posibilidad a las redes inalámbricas a ejecutar aplicaciones de video conferencia de mejor manera. Los canales en 802.11a operan en un ancho de banda de 20 MHz y cada canal está compuesto por 52 subportadoras con un espaciamiento de 0.3125 MHz, de las 52 subportadoras, 48 son de datos y 4 son subportadoras piloto.

En 802.11a se tienen 8 canales disponibles, que no se sobrelapan entre si y se puede instalar hasta 8 equipos en la misma área de cobertura, incrementando la velocidad máxima a 432 Mbps del área cuando se tienen mucha densidad de usuarios.

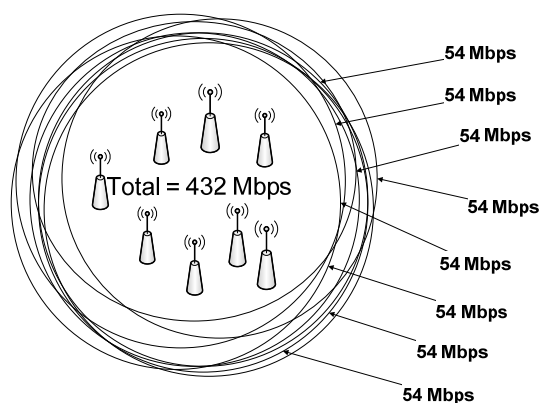


Figura 2-4: Escalabilidad 802.11a

Como 802.11a no trabaja en la misma banda de frecuencias (banda *S-ISM* a 2.4 GHz), donde se tiene muchos equipos electrónicos, tales como: teléfonos inalámbricos, hornos microondas, etc.; que pueden hacer interferencia, 802.11a ofrece mejores velocidades y una señal más limpia. Trabaja con Selección Adaptiva de Velocidad; cuando las características del medio de transmisión no son las mejores se disminuye la velocidad hasta tener una tasa de error aceptable. La velocidad puede variar como: 54, 48, 36, 24, 18, 12, 9, 6 Mbps si es requerido.

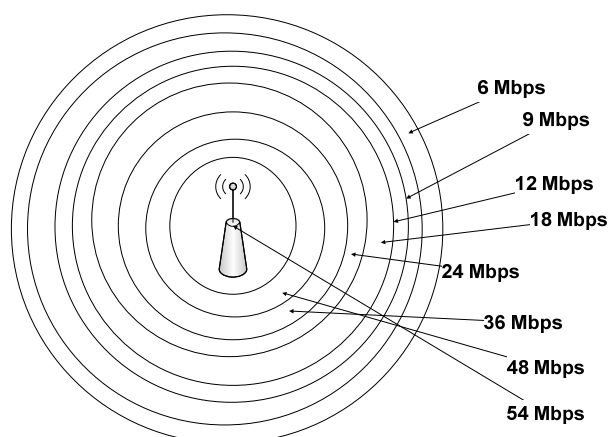


Figura 2-5: Capacidad de Transmisión Vs. Distancia 802.11a

2.2.3.3 Redes Inalámbricas de Área Local IEEE 802.11b

El protocolo 802.11b fue estandarizado en 1999, trabaja en la banda de los 2.4 GHz y opera a una velocidad máxima de 11 Mbps, con una velocidad efectiva promedio de 4 Mbps. Es una extensión de 802.11 con esquema DSSS. 802.11b tiene 3 tipos de modulación, según su velocidad:

- *Binary Phase Shift Keying (BPSK)*
- *Quadrature Phase Shift Keying (QPSK)*
- *Complementary Code Keying (CCK)*

802.11b utiliza CSMA/CA como método de acceso al medio, al igual que el estándar original. La tasa *chipping* de 802.11b es de 11 Mchips, igualmente que 802.11 por lo que ocupa la misma capacidad de transmisión. 802.11b

proporciona velocidades mayores que su predecesor, 5.5 *Mbps* y 11 *Mbps*. Para esto se utiliza el esquema de modulación *CCK*. Debido al *overhead* del protocolo *CSMA/CA*, en la práctica las velocidades de 802.11b para *TCP* es 5.9 *Mbps* y para *UDP* 7.1 *Mbps*.

Este estándar se utiliza en configuración punto a multipunto; un *access point* se comunica con uno o más usuarios de la red localizados dentro de su cobertura. Las velocidades varían según la distancia al *access point*, en interiores a 30 metros se tiene una velocidad de 11 *Mbps* generalmente, y a 90 metros se tiene una velocidad de 1 *Mbps*. En la Figura 2-6 se grafica cómo varía la velocidad según la distancia de los usuarios.

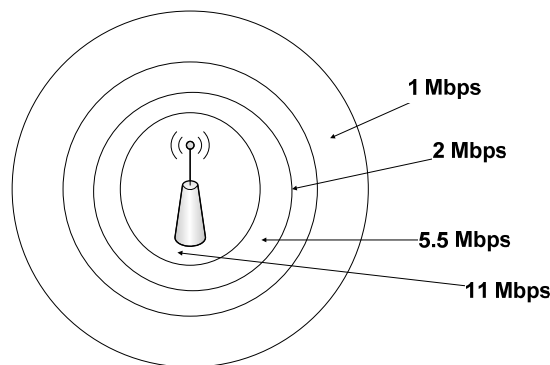


Figura 2-6: Capacidad Vs Distancia 802.11b

La capacidad promedio es compartida dinámicamente con todos los usuarios en un canal. Para incrementar la velocidad de acceso a la red donde exista mucha densidad de usuarios se puede configurar los *access points* en diferentes canales para que no exista interferencia entre ellos. En 802.11b se tienen disponibles once canales para América de los cuales tres no interfieren entre ellos, éstos son: canal 1, 6 y 11.

Con esta técnica al instalar 3 *access points* en una misma área se puede alcanzar una velocidad máxima teórica de 33 *Mbps* y brindar mayor velocidad por usuario o soportar más usuarios por área, como se muestra en la Figura 2-7.

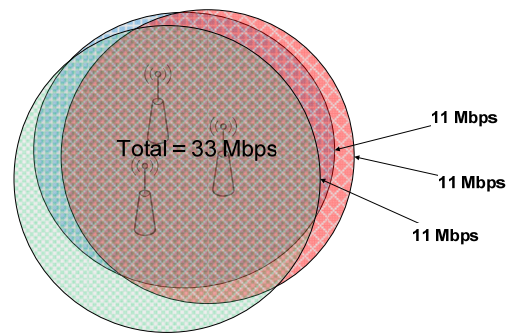


Figura 2-7: Escalabilidad 802.11b

Las tarjetas de red inalámbricas que trabajan bajo el estándar 802.11b pueden operar a 11, 5, 2 o 1 *Mbps* según las condiciones del lugar. Esta tecnología disminuye la velocidad para tratar de disminuir los errores, hasta que se logra un servicio estable a una velocidad determinada, y se llama Selección Adaptiva de Velocidad.

2.2.3.4 Redes Inalámbricas de Área Local *IEEE 802.11g*

El protocolo 802.11g fue estandarizado en junio 2003, el mismo que trabaja en la banda de 2.4 *GHz* y opera a una velocidad máxima de 54 *Mbps*, con una velocidad efectiva promedio de 19 *Mbps*. Los equipos que cumplen con el estándar 802.11g son totalmente compatibles con los del estándar 802.11b, para garantizar interoperabilidad hacia atrás.

El esquema de modulación que se maneja es *OFDM*, para las velocidades de 6, 9, 12, 18, 24, 36, 48 y 54 *Mbps* y por compatibilidad con el estándar 802.11b se maneja la modulación *CCK* para velocidades de 5.5 y 11 *Mbps* y la modulación *BPSK / QPSK / DSSS* para velocidades de 1 y 2 *Mbps*. A pesar de que 802.11g opera en el mismo rango de frecuencias que 802.11b puede manejar mayores velocidades por el esquema de modulación *OFDM*. En la Figura 2-8 se observa las variaciones de las velocidades de este estándar según la distancia.

En el año 2003 los fabricantes de equipos de conectividad presentaron versiones *draft* de equipos 802.11g, antes de que el estándar fuera ratificado; por la intensa competencia entre los fabricantes se tuvieron que bajar los costos de fabricación. Después de la ratificación del estándar salieron al mercado tarjetas de red compatibles con los estándares 802.11 a/b/g, las llamadas tribanda que eran compatibles con todos los equipos como: *access points*, ruteadores inalámbricos, etc.

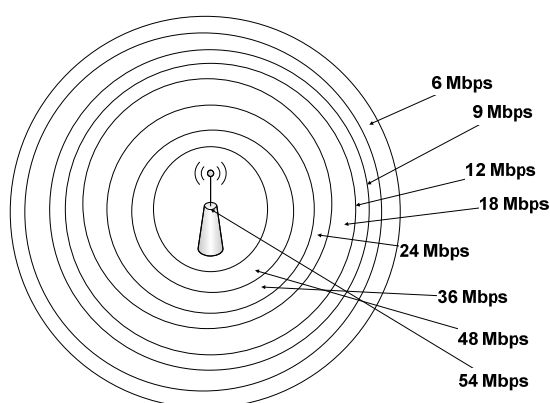


Figura 2-8: Capacidad Vs. Distancia 802.11g

802.11 b y g puede tener implementaciones con más de un *access point* en la misma área de cobertura para incrementar la velocidad máxima cuando se tiene mucha densidad de usuarios en la misma área. 802.11g también trabaja con 3 canales que no se sobrelapan, por lo tanto se puede instalar un máximo de tres *access point* por área.

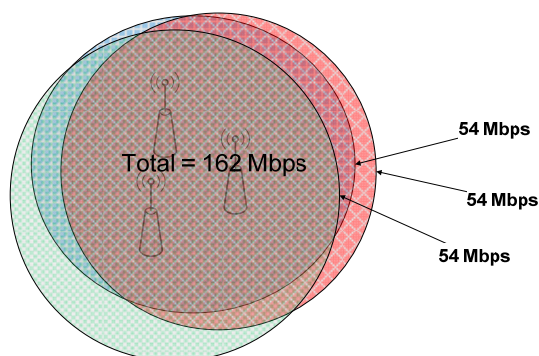


Figura 2-9: Escalabilidad 802.11g

Al operar 802.11g en la misma banda de frecuencia que 802.11b se tienen los mismos problemas de interferencia con algunos artefactos electrónicos que trabajan en la misma banda de frecuencia, pero a pesar de esto y por sus varias bondades es el estándar de redes más usado actualmente.

2.2.3.5 Cuadro Comparativo Tecnologías de Redes Inalámbricas

Estándar	802.11a	802.11b	802.11g
Velocidad Máxima	54 Mbps	11 Mbps	54 Mbps
Rango	8 a 23 metros	30 a 45 metros	30 a 45 metros
Frecuencia	5.8 GHz una banda no muy utilizada	2.4 GHz una banda saturada por equipos electrónicos.	2.4 GHz una banda saturada por equipos electrónicos.
Aceptación	Los equipos con este estándar no son muy comunes, son más utilizados en usuarios corporativos.	Algunos <i>Hot spots</i> están ya instalados con este estándar y existen bastantes equipos funcionando.	Compatible con el estándar 802.11b por lo que pueden coexistir con redes de este estándar.

Tabla 2-3: Comparación Estándares 802.11

2.2.4 TECNOLOGÍAS PARA SISTEMAS DE TELEFONÍA IP

Telefonía *IP* es un grupo de recursos que hacen posible que una señal de voz viaje a través de *Internet* utilizando el protocolo *IP*. La señal de voz viaja digitalizada y empaquetada en paquetes *IP* por la red *Internet*.

Lo más atractivo de la Telefonía *IP* son los bajos costos con relación a la telefonía convencional, por los costos que las operadoras de telefonía pública cobran por las llamadas de larga distancia.

Otros ahorros se dan al utilizar la misma red para voz y datos, cuando los usuarios no utilizan toda la capacidad de su red de datos ya implementada, entonces se puede implementar Telefonía *IP* sin una inversión muy alta.

Generalmente las llamadas entre usuarios de *VoIP* son “gratuitas”¹⁴, pero si se realiza una llamada entre *VoIP* y *PSTN* se tiene un costo que depende a donde se esté llamando, pero este es más bajo que llamar desde la *PSTN* normalmente. Hay dos tipos de servicios de *PSTN* a *VoIP*:

- Llamadas Locales Directas (*DID*) conecta a quien hace la llamada directamente con el usuario de *VoIP*
- Números de acceso, requiere que se introduzca el número de extensión del usuario de *VoIP*; los números de acceso son usualmente cobrados como una llamada local para quien realizó la llamada desde la *PSTN* y es gratis para el usuario *VoIP*.

2.2.4.1 Funcionalidades Telefonía *IP*

- Las llamadas telefónicas pueden enrutarse automáticamente a un teléfono *IP*, sin importar el lugar donde se conecte a *Internet*. Por ejemplo, si el usuario de *VoIP* sale de viaje puede recibir sus llamadas en cualquier lugar siempre y cuando esté conectado a *Internet*.
- Existen números telefónicos gratuitos para *VoIP* en Estados Unidos, Reino Unido, etc.
- En los *call center* los trabajadores pueden atender sus llamadas en cualquier lugar donde tengan una buena conexión de *Internet*.
- Existen servicios de valor agregado en la Telefonía *IP* que son gratuitos, como: conferencias de tres usuarios, retorno de llamada, remarcación automática, identificación de llamadas, entre otros servicios que la operadora de la *PSTN* cobraría un cargo extra.

¹⁴ Desde el punto de vista que no se paga nada por el servicio de Telefonía en algunos sistemas de Telefonía *IP*.

2.2.4.2 Movilidad

La movilidad que brinda la Telefonía *IP* a sus usuarios es uno de los atractivos de esta tecnología. A continuación se detallan algunas ventajas:

- Los usuarios de la Telefonía *IP* pueden hacer y recibir llamadas locales fuera de su localidad. Por ejemplo si un número es de Ecuador y el usuario está viajando a Estados Unidos, se recibirá la llamada en Estados Unidos pero se cobrará como una llamada local, porque la llamada se la realizó desde Ecuador. Igualmente si al usuario de Ecuador le llaman desde Estados Unidos a Ecuador, el que realizó la llamada paga como llamada local.
- Los usuarios de Mensajería Instantánea basado en *VoIP* pueden viajar a cualquier lugar del mundo y hacer o recibir llamadas telefónicas.
- Los teléfonos *IP* pueden integrarse a otro tipo de servicios como video llamadas, intercambio de datos y mensajes, audio conferencias, etc.

2.2.4.3 Ventajas de la Telefonía *IP*

- Es una solución escalable y versátil, ya que se puede incrementar las extensiones *IP* sin mucha inversión utilizando la red de datos.
- Puede ser implementado tanto en hardware como en *software*, para usuarios que no están muy familiarizados con los computadores es más fácil porque ya están familiarizados con los teléfonos para hablar.
- Permite la integración de video conferencia.
- Da mayor movilidad a los usuarios, si alguien se cambia de lugar solo lleva su teléfono y listo, no tiene que cambiar la configuración.
- Telefonía para tele-trabajadores, solo se necesita una conexión a *Internet* para que sus empleados se conecten a las centrales telefónicas de la empresa y reciban sus llamadas.
- Ahorro de recursos al no tener una red de datos y una de telefonía, no se tiene dos tipos de cableados y dos técnicos o grupos de técnicos para dar soporte a dos tipos de redes.

2.2.4.4 Arquitectura Telefonía IP

La arquitectura para la telefonía *IP* es básica y muy parecida a la que tiene la *PSTN*, a continuación se describen las partes de la arquitectura:

- **Terminales:** son los teléfonos *IP* o los programas que los sustituyen y actúan como herramientas para la comunicación.
- **Gatekeepers:** son el reemplazo de las centrales telefónicas convencionales que se usan en la *PSTN*. Las centrales telefónicas *IP* son totalmente digitales que brindan valores agregados a sus usuarios.
- **Gateway:** es el enlace con la red telefónica convencional para tener comunicación con los teléfonos convencionales.

Esta estructura puede ser utilizada para interconectar las sucursales de una misma empresa, con la ventaja de que todas las comunicaciones serían gratuitas y a medida que pasa el tiempo más empresas y personas utilizan esta tecnología lo que abarataría costos porque serían gratis las llamadas entre las empresas y personas que trabajen con *VoIP*.

2.2.4.5 Protocolos de Telefonía IP

Los protocolos para Telefonía *IP* son los siguientes:

- **H.323**, este estándar proporciona una base para comunicaciones de audio, video y datos a través de una red *IP*, que no proporciona *QoS*. Los productos que cumplen con este estándar pueden interoperar con productos de otras marcas. *H.323* tiene una gran cantidad de dispositivos específicos y tecnologías embebidas en ordenadores personales, para comunicación punto a punto o conferencias multipunto. *H.323* tiene control de llamadas, gestión multimedia y de la capacidad de transmisión.
- **Session Initiation Protocol (SIP)**, es un protocolo para la inicialización, modificación y finalización de sesiones interactivas de usuario, como

voz, video, mensajería instantánea, juegos en línea y realidad virtual. *SIP* fue aceptado como protocolo de señalización de *3GPP* y elemento de la arquitectura *IP Multimedia Subsystem (IMS)*. *SIP* es un protocolo para señalización para *VoIP*, junto a *H.323*.

- *Media Gateway Control Protocol (MGCP)*, es un protocolo tipo cliente-servidor de *VoIP*, (*RFC 3435*). Se compone de tres sistemas: *Media Gateway Controller (MGC)*, realiza el control de la señalización *IP*; *Media Gateway (MG)*, realiza la conversión del contenido multimedia; y *Signaling Gateway (SG)*, controla la señalización de la red de conmutación de circuitos. Su sucesor es *Megaco*.
- *Megaco o H.248*, define el mecanismo de llamada para controlar a un *Media Gateway* para llamadas de voz/fax entre redes *RTC-IP* o *IP-IP*, se describe en la *RFC 3525*. *H.248* controla el *Media Gateway* y *H.323* y *SIP* se encargan de comunicarse con otros *Media Gateway*.
- *QSIG*, es un protocolo de señalización entre centrales *PBX* en una Red Privada de Servicios Integrados. Tiene dos capas, que son:
 - Llamada Básica (*BC*): describe la configuración para llamadas entre las *PBXs*.
 - Función Genérica (*GF*): proporciona servicios suplementarios para ambientes empresariales y gubernamentales.

2.2.4.6 Codecs para Compresión de Voz Digitalizada

Los *codecs* para compresión de voz digitalizada más utilizados por las centrales telefónicas *IP* son:

- *G.711* es el primer estándar de la *ITU-T* para voz digitalizada que fue liberado en 1972; para el muestreo utiliza la frecuencia de 8 *KHz* dando una velocidad de bits de la señal codificada de 64 *Kbps*. Este estándar tiene la mejor *MOS*¹⁵ de todos los *codecs* con 4.3. Los pasos para digitalizar la voz son: muestreo, cuantización y Codificación.

¹⁵ *Mean Opinion Score (MOS)*, es decir en español Puntaje promedio de opinión.

Para el proceso de digitalización, existen dos cuantizadores:

- Ley μ se utiliza en Estados Unidos y Japón.
- Ley A se utiliza en Europa, América del Sur y el resto del mundo.

Luego de la cuantización *PCM* los convierte en 8 *bits* por muestra y por último se codifica la voz mediante Códigos de Línea.

- *G.723.1* es un *códec* de audio para voz comprimida. *G.723.1* es totalmente diferente a *G.723*. Tiene dos velocidades operables:
 - *G.723.1* a 6.3 *Kbps* usa el algoritmo de *MPC-MLQ*¹⁶, con tramas de 24 *Bytes* de 30 ms cada una y tiene un *MOS* 3.9
 - *G.723.1* a 5.3 *Kbps* usa el algoritmo de *ACELP*¹⁷, con tramas de 20 *Bytes* de 30 ms cada una y tiene un *MOS* de 3.65
- *G.729* usado en aplicaciones *VoIP* por su bajo requerimiento de capacidad; opera a 8 *Kbps* pero hay variaciones que operan a 6.4 *Kbps* y 11,8 *Kbps*, la primera con menos calidad que la segunda.
 - *G.729a* es compatible con *G.729* pero tiene menos complejidad el algoritmo y por lo tanto la calidad es menor a la de *G.729*.
 - *G.729.1* es una extensión de *G.729* para conversaciones de voz de banda ancha, trabaja en un rango de frecuencias de 50 *Hz* a 7 *KHz*, soporta 8 y 16 *KHz* de frecuencia de muestreo. Tiene una capacidad de 8 a 32 *Kbps* estructurada en 12 capas: 1era. 8 *Kbps*; 2da. 12 *Kbps*; 3era. 14 *Kbps*; las demás capas aumentan 2 *Kbps* por capa.

2.2.4.6.1 Puntuación Media de Opinión (MOS)

Provee una cuantificación numérica de la calidad percibida o recibida de los medios después de la compresión o transformación. Este índice es expresado del 1 al 5, donde 1 es la más baja calidad y 5 es la más alta calidad. Este índice está estandarizado en la recomendación *ITU-T P800*.

¹⁶ *Multipulse LCP with Maximum Likelihood Quantization*

¹⁷ *Algebraic Code Excited Linear Prediction*

CODEC	MOS
G.711 (64 Kbps)	4.3
G.723.1 (6.3 Kbps)	3.9
G.723.1 (5.3 Kbps)	3.65
G.729 (8 Kbps)	3.92
G.729a (8 Kbps)	3.7

Tabla 2-4: MOS de los Codecs VoIP

2.2.5 TECNOLOGÍAS PARA VIDEOCONFERENCIA EN REDES IP

El estándar *H.323* es utilizado para videoconferencia en redes *IP*, para proporcionar una alta calidad. *H.323* es independiente del transporte, permitiendo su implementación en cualquier tipo de red *IP*.

H.323 tiene algunos elementos para una videoconferencia que son:

- Terminales, son los video teléfonos que deben soportar *codecs* de voz y video. Éstos pueden ser implementados tanto en *hardware* como en *software* y existen algunas marcas que los fabrican o desarrollan.
- *Gateway*, es necesario para comunicarse con otras redes, y éste traduce los *codecs* de audio y video usados en ambas redes, procesa la configuración de la llamada.
- *Gatekeepers*, son el punto central de todas las llamadas dentro de una zona, gestionan la capacidad y si se lo supera no se permite mas comunicaciones para no saturar el canal posibilitando la continuidad de servicios como: correo electrónico, transferencia de archivos, etc.

Al tener esta independencia no es necesaria una capa para QoS, por esta razón se desarrolló un protocolo llamado *Resource Reservation Protocol (RSVP)* para suplir las necesidades del transporte en tiempo real.

RSVP es la transición a una nueva arquitectura para asegurar las comunicaciones multipunto en tiempo real, manteniendo la filosofía del protocolo *IP* del mejor esfuerzo. Los puntos básicos para *RVSP* son:

- Establece y mantiene un camino para flujo de datos mediante los protocolos de encaminamiento multipunto.
- Establece un módulo de control que gestiona los recursos de la red.
- Ordena los paquetes en la cola de espera para proveer de la calidad de servicio solicitada.

2.2.5.1 Codecs para Video

2.2.5.1.1 H.263

H.263 es un estándar de codificación de video diseñada por la *ITU-T* en 1995-1996, como un formato comprimido de baja demanda de capacidad para videoconferencia. Fue diseñado para ser utilizado en sistemas basados en la *PSTN*, pero en la actualidad es utilizado con *H.323*, *H.320*, *RSTP* y *SIP*.

H.263 tiene tres versiones: la primera fue terminada en 1995, la segunda, *H.263+* o *H.263 v2* en 1998 y la tercera versión, *H.263++* o *H.263 v3* en el año 2000.

H.263 es utilizado en algunas aplicaciones como:

- *H.263* puede ser decodificado en librerías gratuitas usadas en programas como: *Mplayer*, *VLC Media Player*, etc.
- La mayoría de contenido de videos *flash* utilizados en: *YouTube*, *Google Video* o *MySpace* están codificados en este formato, ya que es soportado por *Macromedia Flash 8*.
- La versión original del códec de *RealVideo* fue basada en *H.263* hasta la versión 8 del programa.

2.2.5.1.2 H.264

H.264 o *MPEG-4* parte 10 define un códec de video de alta compresión, desarrollado por la *ITU-T Video Coding Experts Group (VCEG)* e *ISO/IEC Moving Picture Experts Group (MPEG)*. Estos dos grupos unidos en el año 2001 se llamaron *Join Video Team (JVT)*, la *ITU-T* lo quiso estandarizar con el nombre de *H.264* y la *ISO/IEC* con el nombre de *MPEG-4* parte 10 Códec de Video Avanzado (*AVC*).

La intención de este proyecto era crear un estándar capaz de brindar imagen de buena calidad utilizando una menor capacidad de transmisión que sus antecesores *MPEG-2*, *H.263* o *MPEG* parte 2. *H.264* está enfocado para video de baja calidad para videoconferencia y aplicaciones de *Internet*.

Este estándar maneja algunas capacidades de transmisión, dados los costos de los servicios de *Internet* o los enlaces de datos. Con el perfil original *H.264* puede manejar una resolución de video de:

- A 192 Kbps:
 - 176 X 144 pixeles a 30.3 cuadros por segundo.
 - 320 X 240 pixeles a 10.0 cuadros por segundo.
- A 384 Kbps:
 - 320 X 240 pixeles a 20.0 cuadros por segundo.
 - 352 X 288 pixeles a 15.2 cuadros por segundo.

2.2.5.2 Videoconferencia una aplicación en tiempo real

A diferencia de otros servicios de la red la videoconferencia es una aplicación de tiempo real, cuando no se tiene una capacidad de transmisión suficiente para ejecutarla se tienen los siguientes problemas:

- Tiempo total de retraso punto a punto (latencia)
- Diferencia de retraso (*Jitter*)

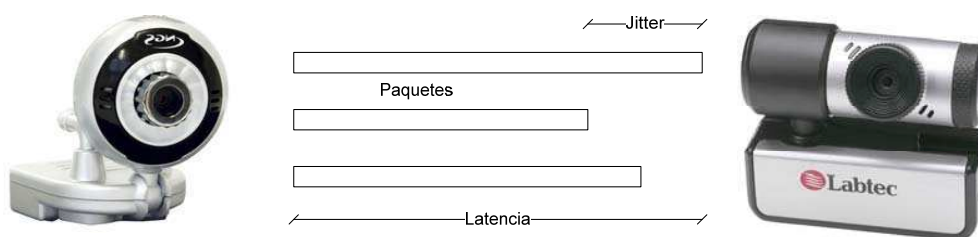


Figura 2-10: Latencia y *Jitter* en Videoconferencia

La pérdida de paquetes también influye en la calidad de la videoconferencia y si es muy notoria puede hacer que la videoconferencia no sea aceptable y solo se escuche el audio. Los efectos de la pérdida de paquetes son:

- Diferencia de retraso de paquetes (*jitter*) puede ocasionar su pérdida.
- Una pérdida de paquetes del 1% del total puede producir una videoconferencia entrecortada con pérdida de audio.
- Una pérdida de paquetes del 2% del total ocasiona una videoconferencia de mala calidad, aunque el audio sea aceptable.
- Una pérdida de paquetes de más del 2% es inaceptable en una conferencia a nivel de empresas.

2.2.5.3 Capacidad Videoconferencia IP

Calidad	Capacidad	Consumo Real de Capacidad
15 cuadros por segundo	128 Kbps	128 Kbps + 25% (<i>overhead LAN</i>) = 160 Kbps
30 cuadros por segundo	192 Kbps	192 Kbps + 25% (<i>overhead LAN</i>) = 240 Kbps

Tabla 2-5: Capacidad necesaria para Videoconferencia IP

Una videoconferencia a 240 Kbps puede variar la resolución dependiendo de los *codecs* de audio y video utilizados. Un equipo de videoconferencia *Polycom* a 240 Kbps utiliza un *códec* de video *H.264* y un *códec* de audio a 32 Kbps y una resolución *Full CIF*¹⁸. A diferencia de un equipo *Aethra* que a la misma capacidad de transmisión utiliza un *códec* de video *H.263* y uno de audio *G.711* a 64 Kbps con una resolución *QCIF*¹⁹.

¹⁸ *CIF* es un estándar que regula la resolución de un cuadro de un video (352 X 288) *pixeles*.

¹⁹ *QCIF* es un estándar que regula la resolución de un cuadro de un video es un cuarto de *CIF* (176 X 144) *pixeles*.

2.3 ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS PARA SEGURIDAD EN REDES²⁰

Una red segura se logra con varios componentes como:

- *Firewalls*
- *Intrusion Detection System (IDS)*
- *Intrusion Prevention System (IPS)*
- Servidores de Autenticación
- Usar *VPNs* para transmitir información en enlaces privados e *Internet*.
- Seguridad para Redes Inalámbricas.

2.3.1 Red Privada Virtual (VPN)

Una *VPN* es extender la red local privada sobre una red pública, ésta puede ser cualquier red de datos incluso la *Internet*. Por ejemplo, cuando se necesita interconectar dos o más sucursales de una empresa, la opción más barata y rápida es utilizar *Internet*. Con esta tecnología se puede implementar un sistema de teletrabajo en la empresa, es decir que el personal se conecte desde su casa a los servidores de forma segura a través de *Internet*.

Para brindar estos servicios se tiene que implementar una política de seguridad en la empresa y garantizar algunos pilares importantes en la seguridad de la red, que son:

- Autenticación, identificado el usuario, se autentica para verificar que es quien dice ser.
- Integridad, mantener la información sin cambios.
- Confidencialidad, mantener la privacidad de la información utilizando encriptación para que nadie puede leer la información sin autorización.

²⁰ Material de Apoyo de "Seguridad en Redes", Ing. Nelson Ávila. EPN

- No Repudio, para implementar esto se debe llevar contabilidad (registro de las actividades de los usuarios), ya que así no pueden negar alguna acción que realizaron.

2.3.1.1 Ventajas de VPNs

Las VPNs se han vuelto populares por las ventajas que ofrecen, éstas son:

- Reducen costos al no tener que contratar enlaces dedicados.
- Privacidad de la información, porque la información va encriptada.
- Flexibilidad en la implementación.
- Escalabilidad en la implementación.
- Acceso seguro a los recursos de la red desde cualquier parte.

2.3.1.2 Requerimientos para Implementar VPNs

- Autenticación, por medio esquemas de usuario y clave, *token cards*, *smart cards*, certificados digitales, etc.
- Autorización, por perfil de usuario, niveles de autorización y acceso.
- Integridad, usando algoritmos de *hashing*, como: *SHA*, *MD5*, etc.
- Contabilidad, registros de la actividad de los usuarios en la red.
- Desempeño, adicionalmente a la seguridad se busca tener tiempos de respuesta como si no se tuviera un esquema de seguridad. Se debe cumplir con: calidad de servicio, acuerdo de niveles de servicio, etc.
- Encriptación de la información, cuando se va a transmitir información en una red pública o el *Internet* debe encriptarse con un método suficientemente seguro, acorde con la importancia de la información.
- Administración de Contraseñas, la política de seguridad de la empresa dice que se deberán cambiar las contraseñas periódicamente y las mismas deben cumplir con los lineamientos de contraseñas fuertes, según su estructura y el número de caracteres.

- Soporte a múltiples protocolos, las *VPNs* deben ser compatibles con el mayor número de protocolos disponibles, por ejemplo *IP*, *IPX*, etc.
- Cumplimiento de estándares y compatibilidad, manejar estándares abiertos de encriptación, intercambio de llaves, etc.
- Facilidad de administración, en cuanto al manejo de direcciones, eventos, auditoría y reportes.

2.3.1.3 Tipos de *VPNs*

Existen tres tipos de *VPNs*, que son los siguientes:

- *VPN de Acceso Remoto Dial UP*, este tipo de *VPN* sirve para dar acceso remoto a empleados, usuarios o proveedores a los recursos de la red de la empresa. Cuando un usuario es autenticado por un servidor *RADIUS* tiene los mismos accesos y privilegios como si estuviera conectado en su oficina.
- *VPN Intranet LAN - LAN*, este esquema es utilizado para interconectar sucursales con la matriz de la empresa. Existe un concentrador de *VPNs* que está conectado a *Internet* y recibe la petición de los equipos de las sucursales para levantar el túnel *VPN*, todas las sucursales deben tener acceso a *Internet* para realizar esta conexión.
- *VPN Extranet LAN – WAN*, se da acceso seguro a usuarios externos o proveedores, debidamente autenticados y autorizados a ingresar a determinado segmento de la red para realizar consultas en los servidores de la *Intranet*.

2.3.1.4 Implementaciones de *VPNs*

Existen tres tipos de implementaciones de *VPNs*, que son las siguientes:

1. Implementaciones en *hardware*, ofrecen mayor rendimiento y facilidad de configuración, no son tan versátiles en cuestión de actualizaciones como las implementaciones en *software*. Algunos fabricantes de

equipos de conectividad ofrecen este tipo de equipos, como por ejemplo: *Cisco*, *3COM*, *Dlink*, entre otros.

2. Implementaciones basadas en *Firewall*, el nivel de protección es bastante bueno pero se sacrifica el rendimiento, ya que el mismo equipo realiza dos funciones simultáneas. Cuando la carga por el manejo de *VPN* es muy considerable se suele instalar un equipo que maneje las *VPN* exclusivamente. Los equipos que cumplen con estas características son: *Checkpoint NG*, *Cisco Pix*, entre otros.
3. Implementaciones en *software*, es la solución más personalizable según las necesidades de la empresa y las más compatibles. Este tipo de soluciones sacrifican el rendimiento de la *VPN* por ejecutarse en un computador, donde se realizan tareas adicionales. Debe ser configurado por un especialista, ya que se debe tomar en cuenta que el *software* de *VPN* se instala sobre un sistema operativo que tiene vulnerabilidades y éstas pueden ser aprovechadas por el atacante para ingresar a la red. Algunos de los programas disponibles para *VPN* son: *OpenSSH*, *OpenVPN*, *FreeS/WAN*, entre otros.

2.3.1.5 Tecnologías para VPNs

Capa Aplicación	<i>Proxy</i> de Aplicación
Capa Presentación	
Capa Sesión	<i>SOCKS v5</i> , <i>SSL</i> , <i>TLS</i>
Capa Transporte	
Capa Red	<i>IPSec</i>
Capa Enlace	
Capa Física	<i>PPTP</i> , <i>L2F</i> , <i>L2TP</i>

Tabla 2-6: Capas del Modelo OSI y Protocolos de Encriptación

La encriptación en *VPN* se puede hacer en cualquiera de las capas del modelo OSI; hay que tomar en cuenta que mientras se necesite mayor seguridad se debe realizar la encriptación en la capa más baja posible. Por ejemplo, si se realiza la encriptación en la capa enlace se logra mayor seguridad, seguida por la encriptación en la capa de red y por último la encriptación en la capa aplicación que no es tan robusta en relación a la seguridad, por permitir visualizar información de: direcciones *IP*, puertos, etc.

La encriptación en la capa de red es la más utilizada por su versatilidad y seguridad, que brinda al no hacerla en capas superiores. Se centrará únicamente la descripción del Protocolo *IPSec*, por ser la mejor opción entre versatilidad y seguridad en la implementación de *VPN*. La encriptación en esta capa no necesita ser soportada por los equipos de red intermedios, es independiente de la topología, del medio de transmisión y de la interfaz.

2.3.1.6 *IPSec*

Es un conjunto de protocolos desarrollado por *IETF* para facilitar el intercambio seguro de paquetes *IP*. *IPSec* trabaja en la capa de red, protegiendo y autenticando paquetes *IP* entre los equipos que mantienen la *VPN*. No está ligado a ningún algoritmo de cifrado, autenticación, manejo de llaves, etc.; permitiendo utilizar cualquier tipo de algoritmos inclusive nuevos algoritmos que se desarrollen en un futuro.

2.3.1.6.1 *Modos de Operación de IPSec*

Soporta dos modos de operación:

- *IPSec* en modo transporte (solo se encripta los datos).
- *IPSec* en modo túnel (encripta todo el paquete)

2.3.1.6.2 *Protocolos de seguridad de IPSec*

Estos protocolos sirven para proteger el contenido de paquetes *IP*, éstos son:

- *Authentication Header (AH)*, brinda autenticación del origen de los paquetes y realiza un chequeo de integridad del mensaje, más no su confidencialidad. El chequeo de integridad se realiza en base a un algoritmo de *hash* como: *MD5* o *SHA*.

- *Encapsulating Security Payload (ESP)*, provee autenticación, confidencialidad e integridad del mensaje. El paquete original es encriptado incluyendo el encabezado con algoritmos como *DES*, *3DES* o algún esquema de encriptación simétrica.

Para el manejo de llaves en *IPSec* se puede utilizar algunos sistemas, como por ejemplo: *Kerberos* o *Internet Key Exchange (IKE)*, este último se utiliza por defecto. *IKE* se encarga del establecimiento y mantenimiento de asociaciones de seguridad.

Para establecer una sesión entre dos dispositivos que soportan *IPSec* se debe realizar la negociación de los parámetros de seguridad, a través de Asociaciones de Seguridad unidireccionales; si se requiere una negociación bidireccional se utilizarán dos Asociaciones de Seguridad.

Las Asociaciones de Seguridad son conexiones unidireccionales que incluyen servicios de seguridad para el tráfico que transportan. La negociación, modificación y eliminación de asociaciones de seguridad se maneja por *Security Association and Key Management Protocol (ISAKMP)*.

2.3.2 FIREWALL

Los *Firewalls* son equipos que se colocan entre dos redes para actuar como puertas por donde todo el tráfico entrante y saliente debe pasar, permitiendo el paso únicamente del tráfico autorizado. Los *firewalls* deben ser muy seguros para que ningún intruso pueda ingresar a la red que está protegiendo, sin ser autorizado.

En la Figura 2-11 se muestra cómo un *firewall* separa dos redes que están directamente conectadas.

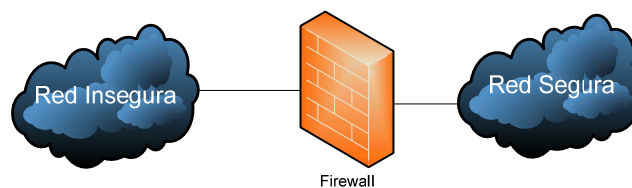


Figura 2-11: Esquema de Implementación de un *Firewall*

2.3.2.1 Ventajas de los *Firewalls*

- El uso de *firewalls* se ha vuelto común en el ambiente empresarial, ya que disminuye los ataques desde redes públicas como el *Internet*, controlando el tráfico no autorizado.
- Permite acceder a *Internet* a los usuarios internos de la red segura.
- El *firewall* está constantemente monitoreando la red para mitigar ataques y en caso de tener uno en curso notificar al administrador vía *email* o por medio de algún tipo de alerta visual o sonora.
- Almacena los registros de los ataques que se han tenido.
- Los *firewalls* tienen la funcionalidad de iniciar o terminar *VPN*, dando un valor agregado a estos equipos.

2.3.2.2 Desventajas de los *Firewalls*

- Los *firewalls* son un único punto de falla, el concepto de un *firewall* es de un equipo conectado entre dos redes para controlar el tráfico entrante y saliente. Para esto solo se debe tener una conexión entre las dos redes para poderla administrar de manera eficiente.
- La implementación y configuración debe hacerla un técnico con mucha experiencia, porque un *firewall* mal configurado es una vulnerabilidad.
- Los *firewalls* incrementan los tiempos de respuesta por el procesamiento que realizan para autorizar la información entrante y saliente. Estos equipos deben ser bien dimensionados para la capacidad de procesamiento que se requiera, para no incrementar mucho los tiempos de respuesta.

2.3.2.3 Clasificación de los *Firewalls*

Los *Firewalls* se pueden clasificar de dos maneras:

- Por la manera de filtrar los paquetes
- *Proxy Servers*

La clasificación de los *firewalls* por la manera de filtrar los paquetes es:

- Modo de Filtrado estático: Los criterios para permitir o negar accesos son estáticos, se basa en: direcciones, protocolos o puertos.
- Modo de Filtrado dinámico: este tipo de filtrado de paquetes puede modificar las reglas para permitir o negar accesos de acuerdo a las necesidades del administrador de la red. Puede ser configurado para permitir tráfico entrante como respuesta a un requerimiento saliente, que es bastante recomendable.

La clasificación de los *Proxy Servers* es la siguiente:

- *Proxy Server* de Aplicación, controlan el establecimiento de conexiones; adicionalmente autentica al usuario, la dirección de origen y de destino, así como el protocolo a usarse.
- *Proxy Server* de Circuito, crea un circuito entre el cliente y el servidor sin tener en cuenta la aplicación que se va a ejecutar; se logra cuando el cliente ejecuta una aplicación especialmente diseñada para esto.

2.3.3 SISTEMA DE ANTIVIRUS DE CORPORATIVO

Las empresas dedicadas a desarrollar sistemas de antivirus, antispías, *antispam*, etc., discriminan dos tipos de mercado para brindar soluciones a medida de los usuarios. Los tipos de usuarios son:

- Para usuarios del hogar y empresas de hogar
- Para usuarios empresariales

Los usuarios empresariales tienen requisitos adicionales a los usuarios del hogar, por esto se han creado los Sistemas de Antivirus Corporativos que tienen características para redes. Los requisitos de este tipo de usuarios son:

- Administración centralizada de actualizaciones automáticas.
- Protección para los servidores, estaciones de trabajo, plataformas de mensajería, *firewalls* y servidores *proxy*.
- Monitoreo centralizado de todos los componentes del sistema.
- Administración de usuarios eventuales, que trabajan desde su hogar o los visitantes que se conectan a la red eventualmente; se permite la implementación de políticas de seguridad unificada en redes heterogéneas, tomando acciones de aislamiento de equipos hasta que cumplan con las políticas para ingresar a la red.
- Soluciones escalables e integrales, la modularidad de estos sistemas incrementan sus servicios según las necesidades de la empresa.
- Protección para comunicaciones vía *email*.
- Protección proactiva del sistema de antivirus y sus módulos adicionales de antiespías, *antispam*, etc.
- Restricción de aplicaciones no autorizadas.
- Actualizaciones independientes cuando algún computador de escritorio o portátil no está conectado al servidor de antivirus de la empresa.

Se debe implementar un Sistema Antivirus Corporativo que cumpla con la mayoría de especificaciones antes mencionadas para precautelar la seguridad de la red, en conjunto con sistemas complementarios de prevención contra intrusos, *firewalls*, entre otros.

Algunos ejemplos de Sistemas de Antivirus Corporativos son:

- *Symantec* Antivirus
- Panda Antivirus Corporativo
- *McAfee* Antivirus Corporativo
- *Trend Micro Office Scan*

2.3.4 SISTEMA DE DETECCIÓN DE INTRUSOS

Un Sistema de Detección de Intrusos (*IDS*) detecta accesos no autorizados a computadores o una red. Los *IDS* son un sistema pasivo de seguridad, porque sólo alertan de un ataque pero no toman acciones contra de éste.

Los ataques pueden ser realizados por *hackers* o por programas hechos para esto. Los *IDS* suelen tener detectores virtuales para prevenir ataques en una red, pero muchas veces estos detectores dan falsas alarmas.

Los *IDS* analizan detalladamente el contenido del tráfico de la red en busca de firmas de ataques conocidos o comportamiento sospechosos, como el escaneo de puertos o paquetes alterados que circulan por la red.

Los *IDS* y antivirus tienen una base de datos de firmas de ataques conocidos, que deben ser actualizadas no tan continuamente como la de un antivirus pero debe actualizarse para prevenir la mayor cantidad de ataques.

Los *IDS* por lo general son incluidos en los *Firewall*, ya que por sí solos son incapaces de detener un ataque. Los dispositivos que incluyen un *Firewall* además de un *IDS*, pueden bloquear los puertos cuando ocurre un ataque.

2.3.4.1 Tipos de *IDS*

- *IDS* de Computador (*HIDS*), es un *IDS* que monitorea un computador.
- *IDS* de Red (*NIDS*), es un *IDS* para red que está monitoreando un segmento de la red a la cual tiene acceso.
- *IDS* Distribuido, maneja el modelo cliente-servidor, tiene detectores (*NIDS*) distribuidos en varios puntos y un *IDS* principal con una base de datos centralizada.

2.3.5 SISTEMA DE PREVENCIÓN DE INTRUSOS

Un *IPS* es un sistema que monitorea la actividad de la red en busca de comportamientos maliciosos o no deseados y reaccionan en tiempo real para bloquear o prevenir un ataque. Cuando un ataque es detectado, se eliminan los paquetes alterados y se permite el paso de los paquetes sin alteraciones.

Los *IPS* toman decisiones de control de accesos basados en el contenido de una aplicación, al contrario de los *firewall* tradicionales que lo realizan por dirección *IP* o por número de puerto. Los *IPS* no tienen una dirección *IP* para monitorear un segmento de red.

2.3.5.1 Tipos de IPS

- *IPS* basado en Computador (*HIPS*), es una aplicación de *IPS* que reside en una dirección *IP*, alojada en un computador
- *IPS* de Red (*NIPS*), es una aplicación o un dispositivo que ejecuta el sistema *IPS*. Este sistema está diseñado para analizar, detectar, reportar y reaccionar con eventos relacionados con la seguridad de la red, eliminando el tráfico malicioso.
- *IPS* de Contenido, inspecciona el contenido de los paquetes para verificar las secuencias, las firmas, para detectar y prevenir ataques.
- *IPS* basados en Análisis de Protocolos, decodifican nativamente los protocolos de la capa aplicación, tales como: *HTTP*, *FTP*, etc. Una vez decodificados los protocolos, el *IPS* analiza las partes de protocolo en busca de comportamientos anómalos, cuando éstos son detectados los paquetes anómalos se descartan.
- *IPS* basado en la Velocidad de la Red, este tipo de *IPS* monitorea y aprende el comportamiento normal, se comparan con estadísticas almacenadas, y si detectan velocidades anormales de tráfico se toman medidas de bloqueo para prevenir ataques.

2.3.6 *WI-FI PROTECTED ACCESS 2 (WPA2)*

WPA2 también llamado Seguridad de Red Robusta (*RSN*). *WPA2* usa el estándar de Encriptación Avanzada (*AES*), que es un sistema de cifrado por bloques muy seguro contra criptoanálisis; no es un sistema de cifrado de flujo de *bits* como *WEP* y *WPA* con *RC4* que fueron criptoanalizados y violentados. 802.11i brinda confidencialidad, integridad y autenticación.

Las redes inalámbricas tienen dos mercados, que son: usuarios del hogar y usuarios empresariales. Los usuarios del hogar desean implementar seguridades a su red inalámbrica para que personas no autorizadas no roben sus recursos, tales como: *Internet*, archivos, etc. Por otro lado, los usuarios empresariales buscan seguridad avanzada para no perder su información y no permitir acceso no autorizado a los recursos de la red corporativa.

Tomando en cuenta estos dos segmentos del mercado de redes inalámbricas se manejan dos esquemas de seguridad en 802.11i, llamados:

- *WPA2 Personal*, maneja una clave compartida por todos los usuarios de la red y utiliza encriptación *AES*.
- *WPA2 Enterprise*, este esquema utiliza un servidor *RADIUS* externo para la autenticación y autorización de los usuarios inalámbricos; dependiendo del servidor *RADIUS* se puede manejar diferentes esquemas de autenticación. Para la encriptación entre el cliente inalámbrico y el servidor *RADIUS* utiliza *AES*.

2.3.6.1 *Arquitectura 802.11i*

La arquitectura 802.11i contiene los siguientes componentes:

- Autenticación 802.1X (requiere un servidor de autenticación *RADIUS*)
- Equipos compatibles con *RSN*, no todos los equipos soportan *RSN* porque necesitan encriptar y desencriptar por medio de *hardware*.
- Encriptación *AES* que soporta claves de 128, 192 y 256 *bits*

2.3.7 AUTENTICACIÓN 802.1X

IEEE 802.1X es un estándar para Control de Accesos de Red basado en puertos, permitiendo la autenticación de dispositivos conectados a un puerto LAN, si la autenticación falla se prohíbe el acceso del dispositivo.

802.1X se basa en el Protocolo de Autenticación Extensible (*EAP*). La autenticación es realizada por el servidor *RADIUS*. Se permite la autenticación de las dos partes, es decir, tanto del cliente como del servidor. Los esquemas de autenticación son: *EAP-TLS*, que se basa en certificados digitales tanto en el cliente y el servidor; y *EAP-MS-CHAPv2*, que maneja nombre de usuario y contraseña en el cliente, un certificado digital en el servidor, para disminuir la complejidad de la implementación y los costos.

802.1X puede ser implementado tanto en redes cableadas como inalámbricas, esto incrementa el nivel de seguridad brindando autenticación y autorización, que son dos pilares fundamentales para la seguridad de la red.

2.4 ANÁLISIS DE ALTERNATIVAS TECNOLÓGICAS DE ADMINISTRACIÓN DE RED²¹

La Administración de Redes es un conjunto de técnicas encargadas de mantener una red operativa, eficiente, monitoreada y con una planificación de crecimiento adecuado y propiamente documentada.

Los objetivos principales de la administración de redes son:

- Garantizar la continuidad de operación mediante el control y monitoreo de la red. Detectar y solucionar problemas registrando información de: tiempos de respuesta, solución y el técnico encargado.

²¹ Material de apoyo Administración de Redes, Ing. Xavier Calderón

- Utilizar eficientemente la red y administrar sus recursos, tanto la capacidad de *Internet* como el de los enlaces entre sucursales.
- Reducir costos mediante la optimización de los recursos de la red.
- Gestionar, documentar los cambios y actualizaciones en la red, para que tengan el menor impacto en la actividad de la empresa.

El sistema de administración de red opera bajo los siguientes principios:

1. Recopilar de información del estado de la red y sus componentes.
2. Realizar un informe de la situación actual de la red, en base a la información recopilada.
3. Ingreso de los datos al sistema de monitoreo.
4. Almacenamiento de los datos recopilados en el centro de control.
5. Análisis de parámetros para obtener conclusiones del estado de la red.
6. Establecimiento de políticas y procedimientos de respuesta a fallas.

Un sistemas de administración de red moderno es un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red, es decir, capaz de brindar soporte para múltiples protocolos de red.

2.4.1 ELEMENTOS DEL SISTEMA DE ADMINISTRACIÓN DE RED

Los elementos de un sistema de administración de red son los siguientes:

- Equipos: son los elementos de más bajo nivel y constituyen los equipos de conectividad, estaciones de trabajo, servidores administrados.
- Agentes: programa o conjunto de programas que recopila información de los equipos que conforman el sistema. El agente transmite información al sistema de administración de red, con datos de:
 - Notificación de fallos.
 - Datos de diagnóstico.
 - Identificador del equipo.
 - Características del equipo.

- Administrador del sistema: Es un conjunto de programas instalados en un servidor para este propósito, donde se dirigen los mensajes que requieren acción o que contienen información del agente.

2.4.2 TIPOS DE SISTEMAS DE ADMINISTRACIÓN DE RED

Existen tres tipos de arquitecturas de los sistemas de administración de red, estos son:

- Simple: desde un equipo donde está instalado el *NMS*²² se administra toda la red.

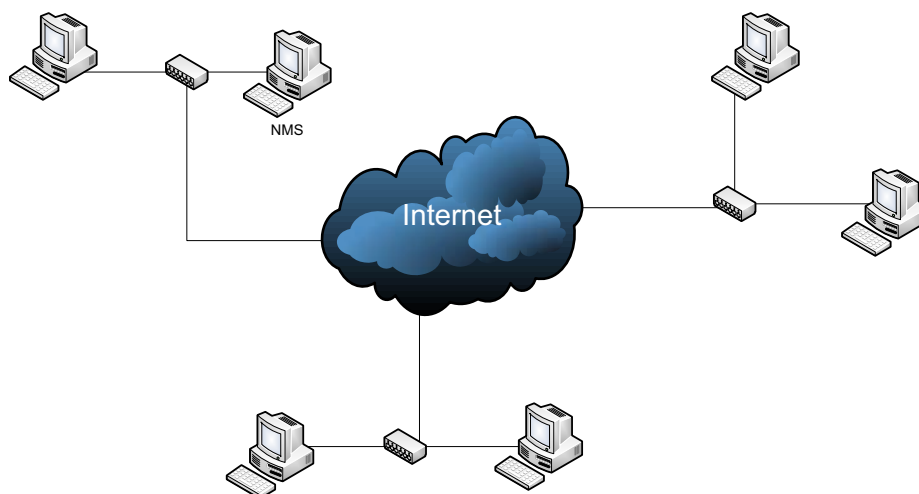


Figura 2-12: *NMS Simple*

- Distribuido: se tienen varios puntos donde se tiene instalado el *NMS*, esta arquitectura es más tolerante a fallas, pero se tiene que consolidar la información de los *NMS*.

²² Sistema de Administración de Red

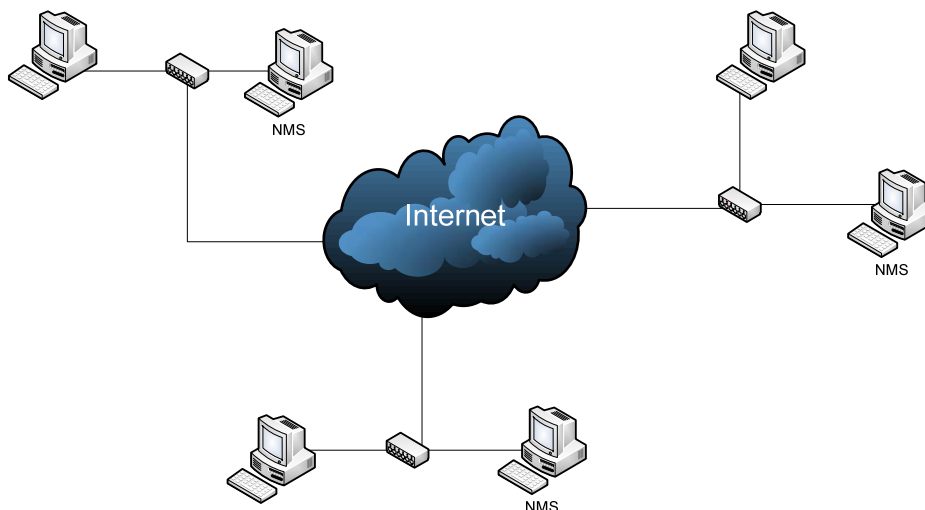


Figura 2-13: NMS Distribuido

- *Web Enterprise Management (WEBEM)*, esta arquitectura es la tendencia de los nuevos NMS. La administración se realiza a través de Internet utilizando el navegador web. Estas aplicaciones están basadas en CGI, Servicios Web, Applets, etc.

Navegador Web
HTTP
Aplicaciones
SNMP

Tabla 2-7: Modelo WEBEM

2.4.3 ALTERNATIVAS PARA LA ADMINISTRACIÓN DE RED

- *Simple Network Management Protocol (SNMP)*: forma parte del grupo de protocolos de Internet fue definido por la IETF, este es usado como sistema de administración de red para monitorear los dispositivos que conforman la red.
- *Common Management Information Protocol (CMIP)*: es un protocolo de administración de red, que proporciona una implementación para

servicios definidos como *CMIS*, que comunican la aplicación de administración de red y sus agentes. Este protocolo nace del modelo de administración de red *ISO/OSI* y está definido por la *ITU-T* en las recomendaciones serie *X.700*.

CMIP administra la información en términos de objetos administrados, permite la modificación y administración de los mismos. Los objetos administrados son descritos usando Guías de Definición de Objetos Administrados (*GDMO*) y son identificados por nombres.

- *Distributed Management Environment (DME)*: Fue desarrollado por *IBM* y *HP*, con el objetivo de crear un sistema escalable e interoperable orientado a objetos. Es capaz de trabajar con cualquier sistema operativo, simplificando la gestión de sistemas distribuidos y *stand alone*, logrando reducir costos de la administración de red.
- *Hyper Media Management Architecture (HMMA)*: es una arquitectura muy versátil que permite administrar una red desde *Internet*, trabaja en conjunto con el protocolo *HTTP* brindando las facilidades de administración remota mediante *web browser*. Esta arquitectura está basada en el protocolo *Hyper Media Management Protocol (HMMP)*, que es el sucesor de *SNMP* pero todavía no está totalmente difundido.

El Protocolo más utilizado para administración de redes y el más compatible con los equipos existentes en la empresa es *SNMP*; los equipos deberán ser compatibles con este protocolo para trabajar con el *Software* de Administración de Red escogido.

Algunos ejemplos de Sistemas de Administración de Red son:

- *Tivoli Netview* de *IBM*
- *SunNet* de *Sun Microsystems*
- *Openview* de *HP*
- *CiscoWorks* de *Cisco*
- *Network Director* de *3COM*

CAPÍTULO 3
ESTUDIO DE REINGENIERÍA
DE LA *INTRANET*

3 ESTUDIO DE REINGENIERÍA DE LA *INTRANET*

3.1 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad son un conjunto de normas que rigen a personas que tienen acceso a la información y equipos de una empresa, con el afán de establecer procedimientos de uso y protección de los sistemas informáticos.

Las políticas de seguridad intentan manejar los riesgos de seguridad a los cuales es susceptible la red y la información organizacional, esto se logra estableciendo políticas y procedimientos de seguridad con apoyo de equipos informáticos que se implementan para cumplir con los estándares requeridos.

La seguridad de la información debe asegurar su confidencialidad e integridad. Los ataques informáticos ponen en peligro la continuidad de la empresa, ocasionando pérdidas económicas y molestias a los clientes por tener que suspender el servicio que brinda la empresa.

Las políticas de seguridad involucran a todo el personal, desde la recepcionista hasta el gerente. La recepcionista registra a los visitantes en una base de datos, esta información es importante para saber quiénes son las personas que han ingresado en caso de tener algún tipo de problema; el gerente tiene información económica y financiera de la empresa que es muy importante, por esto se debe salvaguardar la información empresarial.

En el desarrollo de las políticas de seguridad deben interactuar el Departamento de Sistemas y la Gerencia para determinar los activos de la empresa (que se quiere proteger). Adicionalmente se debe capacitar a los demás empleados para que conozcan las políticas de seguridad y los procedimientos que deben seguir para prevenir y responder ante ataques.

3.1.1 DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA RED

3.1.1.1 Activos a Proteger

- Sistema Integrado de Administración Corporativa.
- Aplicación de la *Intranet*.
- Bases de datos.
- Servidores.
- Equipos de conectividad.
- Licencias de *Software*.
- Respaldos de Bases de datos.
- Respaldos de la información del Sistema Integrado de Administración Corporativa.

3.1.1.2 Vulnerabilidades

- Claves débiles o ausencia de claves para acceso a los equipos y/o servicios de la *Intranet*.
- Configuración por defecto de los equipos de conectividad.
- Falta de seguridad física, no existen cuartos de telecomunicaciones con control de acceso a los equipos de conectividad en las sucursales.
- Falta de seguridad lógica en la *Intranet*, no existe *hardware* o *software* tales como: *Firewalls*, *IDS*, *IPS*.
- No se ha segmentado la red, permitiendo que cualquier usuario o algún intruso pueda acceder a toda la red sin restricciones.

3.1.1.3 Posibles Amenazas

- Ataques Internos, según las estadísticas más del 80% de los ataques conocidos a las *Intranets* corporativas son ataques internos. Los

ataques internos en Tecnomega sí se han dado, principalmente el robo de información de las bases de datos de clientes e inventario.²³

- Ataques Externos, son los que se originan desde *Internet*.

3.1.1.4 Riesgos

- Pérdida de la información por daños en los servidores.
- Fugas de la información, por personal de la empresa.
- Pérdida o mala manipulación de equipos de conectividad.
- Pérdida o mala manipulación de servidores.
- Pérdida o mal uso de los respaldos de bases de datos.
- Pérdida o mal uso de la información del *SIAC*.
- Pérdida de las licencias de *software* que maneja la empresa.

3.1.1.5 Desarrollo de las Políticas de Seguridad

- ❖ **Política:** Las claves de acceso al dominio deben tener como mínimo 8 caracteres alfanuméricos, siguiendo el siguiente formato: cuatro letras y cuatro números.
 - **Propósito:** Manejar claves de acceso robustas para que no sean fácilmente rotas por medio de métodos de fuerza bruta.
 - **Cobertura:** Esta política se aplicará a todo el personal que tenga acceso a la *Intranet* de la empresa.
 - **Cumplimiento:** Se cumplirá esta política si los usuarios tienen claves de 8 caracteres alfanuméricos como mínimo, con 4 letras y 4 números.
 - **Penalidades:** El incumplimiento no permitirá el acceso al sistema.

²³ Estadística obtenida del Material de Apoyo de “Seguridad en Redes”, Ing. Nelson Ávila.
EPN

- ❖ **Política:** Las contraseñas deben ser cambiadas mensualmente o cuando se tenga algún indicio que la contraseña ha sido robada.
 - **Propósito:** Cambio de claves para disminuir el tiempo de vulnerabilidad si una clave es descifrada o robada.
 - **Cobertura:** Esta política se aplicará a todo el personal que tenga acceso a la *Intranet* de la empresa.
 - **Cumplimiento:** Se cumplirá esta política si los usuarios cambian sus claves de acceso cada mes o cuando existan indicios de que ha sido robada.
 - **Penalidades:** No se permitirá el acceso al sistema si la clave de acceso tiene más de un mes de antigüedad.

- ❖ **Política:** Si un usuario ingresa erróneamente su clave más de tres veces, su cuenta quedará bloqueada por una hora. Solamente el Jefe de Sistemas puede desbloquear estas cuentas antes de una hora.
 - **Propósito:** Dificultar el rompimiento de contraseñas con métodos de fuerza bruta.
 - **Cobertura:** Todos los usuarios que tengan acceso a la *Intranet* por medio de una clave de acceso.
 - **Cumplimiento:** Se cumplirá esta política si se bloquean las cuentas con más de tres intentos fallidos de ingresar su clave de acceso y solo el Jefe de Sistemas desbloquea estas cuentas por este problema.
 - **Penalidades:** No se permitirá el acceso a la *Intranet* cuando se ingresa erróneamente la clave de acceso. Se amonestará por escrito a la persona que no siendo el Jefe de Sistemas desbloquee una cuenta bloqueada y de reincidir tendrá una sanción económica.

- ❖ **Política:** El uso del correo electrónico es exclusivamente para cuestiones relacionadas con actividades de trabajo, no para el envío de cadenas u otra información que distraigan al personal de sus actividades.
 - **Propósito:** Utilizar la capacidad de los servidores de correo solamente con información importante para la empresa.

- **Cobertura:** Esta política se aplicará a todo el personal que tenga una cuenta de correo electrónico de la empresa.
 - **Cumplimiento:** Se cumplirá esta política si no se tiene correo basura que sea enviado desde algún *email* del dominio de la empresa.
 - **Penalidades:** Se bloqueará la cuenta de correo electrónico si se identifica desde la cual se está enviando correo basura.
- ❖ **Política:** El acceso a *Internet* debe ser controlado, bloqueando páginas que distraigan a los empleados, páginas de correo electrónico diferente al de la empresa, *chat* o páginas con contenidos sexuales.
- **Propósito:** Aprovechar la capacidad de *Internet* para cosas positivas, que no distraigan a sus empleados.
 - **Cobertura:** Esta política se aplicará a todo el personal que tenga acceso a *Internet* de la empresa.
 - **Cumplimiento:** Se cumplirá esta política si dentro de los registros del *firewall* no se encuentran accesos a las páginas *web* restringidas o prohibidas en la organización.
 - **Penalidades:** Se amonestará verbalmente al empleado que infringiere esta política, y se reincide se le suspenderá el acceso a *Internet*.
- ❖ **Política:** Cualquier tipo de ataque interno a la integridad, privacidad y confidencialidad de la información empresarial está totalmente prohibido, igualmente atentar contra la continuidad del funcionamiento de los sistemas informáticos de la empresa.
- **Propósito:** Mitigar los ataques internos que afecten en la actividad de la empresa y a sus activos.
 - **Cobertura:** A todos los empleados de la empresa.
 - **Cumplimiento:** Se cumplirá esta política cuando no se produzcan ataques internos comprobados por las herramientas de seguridad que estén al alcance de técnicos que investiguen el origen del ataque.
 - **Penalidades:** Se separará de la empresa a la persona que se le comprobare haya realizado un ataque contra la infraestructura informática y de telecomunicaciones de la empresa.

- ❖ **Política:** Manejo de datos e información empresarial de acuerdo al grado de importancia y sensibilidad de la misma.
 - **Propósito:** Dar la importancia necesaria a la información empresarial que se maneja día a día para el funcionamiento de la organización.
 - **Cobertura:** A todos los empleados de la empresa que manejen cualquier tipo de información privada de la empresa.
 - **Cumplimiento:** Se cumplirá esta política cuando no existan fugas de información de las bases de datos de la empresa.
 - **Penalidades:** Quien divulgare información confidencial o privada será multado económicamente la primera vez y la segunda vez será separado de la empresa.

- ❖ **Política:** La administración de la infraestructura de red, *Intranet* y equipos de computación será realizada por el Departamento de Sistemas. Dentro de la administración está la creación de cuentas de usuario, la asignación de permisos, realización de auditorías, registros, respaldos de las aplicaciones e información empresarial y la documentación de los cambios de configuración en equipos y programas.
 - **Propósito:** Determinar las funciones del Departamento de Sistemas con respecto a las políticas de seguridad.
 - **Cobertura:** A todos los empleados del Departamento de Sistemas.
 - **Cumplimiento:** Se cumplirá esta política cuando el Departamento de Sistemas administre la red, *Intranet* y los equipos de computación, guardando registros y documentación.
 - **Penalidades:** El empleado que no cumpliera con esta política una vez tendrá una amonestación verbal y si se vuelve a repetir tendrá una amonestación por escrito con una multa económica.

- ❖ **Política:** El acceso remoto de usuarios registrados a la *Intranet* debe cumplir con esquemas de seguridad, tales como: autenticación y control de acceso.
 - **Propósito:** Incrementar la seguridad de la red controlando los accesos remotos que suelen ser un hueco de seguridad.

- **Cobertura:** A todos los empleados de la empresa que tengan claves de acceso remoto a la *Intranet* y al Departamento de Sistemas que es el que administra las claves de estos usuarios.
 - **Cumplimiento:** Se cumplirá esta política cuando se tenga un acceso remoto controlado y seguro, donde todos los usuarios tengan que autenticarse para acceder a la *Intranet* y se establezca control de accesos.
 - **Penalidades:** No se permitirá el acceso a los usuarios no registrados, y se bloqueará el acceso cuando se detecte que el usuario está realizando acciones que puedan poner en peligro a la *Intranet*.
- ❖ **Política:** Las redes inalámbricas implementadas deben tener un esquema de seguridad *WPA2 Enterprise* la cual utiliza un servidor *RADIUS* para la autenticación. Los *Hot Spots* instalados en las sucursales de la empresa son los únicos que podrán no tener clave de acceso, pero tendrán acceso a la red de la empresa.
- **Propósito:** Para mantener un alto nivel de seguridad en la red tanto inalámbrica como cableada.
 - **Cobertura:** A todas las redes inalámbricas instaladas en las sucursales de la empresa.
 - **Cumplimiento:** Se cumplirá esta política cuando todas las redes inalámbricas cumplan con el estándar de encriptación y autenticación que se especifica, solo los *Hot Spots* están exentos de estas medidas de seguridad.
 - **Penalidades:** Se notificará del incumplimiento de esta política al Jefe de Sistemas y de reincidir será amonestado por escrito el encargado de la sucursal.
- ❖ **Política:** La red tendrá un dominio implementado que: administre cuentas de usuario y grupos de usuarios; control de accesos a grupos de usuarios o usuarios específicos, administre recursos compartidos, impresoras, etc.; instale actualizaciones de sistemas operativos, etc.

- **Propósito:** Diferenciar los tipos de usuarios y designar tareas específicas a cada grupo y su responsabilidad con la seguridad.
 - **Cobertura:** Todos los usuarios con acceso al dominio de la red.
 - **Cumplimiento:** Esta política se cumplirá cuando todos los usuarios estén agrupados dentro un perfil de grupo, que esté de acuerdo con su función y necesidades de acceso.
 - **Penalidades:** Se bloqueará las cuentas de los usuarios que hagan mal manejo de las mismas, tal como: cambiar su grupo de usuario, utilizar cuentas de otros usuarios o crear cuentas con perfiles diferentes a los determinados por el Departamento de Sistemas. Si se reincide en la falta se impondrá una sanción económica determinada por la gravedad de la falta.
- ❖ **Política:** Los equipos de conectividad, telefonía y los servidores deben estar instalados en cuartos de telecomunicaciones con acceso restringido; éste debe ser controlado por tarjeta magnética o controles biométricos.
- **Propósito:** Permitir el acceso exclusivamente al personal autorizado para proteger los equipos y garantizar su funcionamiento.
 - **Cobertura:** A todos los empleados de la empresa.
 - **Cumplimiento:** Se cumplirá esta política cuando todas las sucursales tengan un cuarto de telecomunicaciones con control de accesos.
 - **Penalidades:** De no cumplirse el estricto control del personal para ingresar a los cuartos de telecomunicaciones, la primera vez se llamará la atención verbalmente al encargado y la segunda vez será por escrito. Si se llegare a afectar a los equipos se tomará acciones legales contra los responsables.
- ❖ **Política:** Todas las configuraciones de equipos de conectividad, centrales telefónicas y servidores deben ser debidamente documentadas, guardadas en formato digital de ser posible, almacenadas en sus respectivos cuartos de telecomunicaciones y entregadas al Jefe de Sistemas.
- **Propósito:** En caso de una emergencia configurar o cargar la configuración de determinado equipo si así se requiere.

- **Cobertura:** A todos los empleados del Departamento de Sistemas.
 - **Cumplimiento:** Se cumplirá con esta política cuando se documente las configuraciones de los equipos y se obtengan las configuraciones en formato digital de ser posible.
 - **Penalidades:** De no tenerse documentada o respaldada la configuración de un equipo se llamará la atención verbalmente al encargado y de repetirse el llamado de atención será por escrito.
- ❖ **Política:** Dada la salida de un empleado de la empresa se cancelará máximo en 24 horas las cuentas de correo, usuario de acceso al dominio, tarjetas magnéticas y registro de controles biométricos de tenerlos.
- **Propósito:** Evitar accesos no autorizados de personal que ya no trabaja en la empresa.
 - **Cobertura:** Al Jefe del Departamento de Sistemas.
 - **Cumplimiento:** Esta política se cumplirá cuando después de la separación de un empleado de la empresa, se elimine todas sus claves de acceso en menos de 24 horas de su salida.
 - **Penalidades:** De no cumplirse el plazo máximo de esta política se amonestará verbalmente y de reincidir se lo hará por escrito.
- ❖ **Política:** Se conformará un equipo de trabajo para la seguridad informática de la empresa con el fin de hacer cumplir, monitorear y reformar las políticas de seguridad.
- **Propósito:** Mantener actualizadas y en uso las políticas de seguridad según las necesidades de la empresa.
 - **Cobertura:** A los miembros del equipo de trabajo para la seguridad informática.
 - **Cumplimiento:** Se ejecutará esta política cuando el equipo de trabajo se encargue de hacer cumplir y monitorear el cumplimiento de las políticas de seguridad, así como de su reforma según las necesidades de la empresa.
 - **Penalidades:** De no cumplirse esta política se amonestará verbalmente y de reincidir se lo separará de este equipo.

3.2 REDISEÑO DE LA RED LAN CABLEADA E INALÁMBRICA

El rediseño de la red de Tecnomega es muy importante para implementar servicios de voz, datos y video con calidad de servicio, es decir manejar una red convergente. Se debe lograr una buena calidad en conversaciones telefónicas por medio de Telefonía *IP*; una videoconferencia fluida con las sucursales de la empresa de otras ciudades u otros países.

Los equipos de conectividad para una red convergente deben cumplir requerimientos especiales como *QoS*, *VLAN* exclusiva para Telefonía *IP*, *PoE*²⁴ (para manejo de energía centralizada). Una red segura necesita características como: *VLANs*, *ACL*²⁵, *Firewall*, *IPS*, respaldo de *UPS*, caminos redundantes, seguridad física de información e infraestructura informática.

Las Centrales Telefónicas *IP* pueden soportar protocolos para Telefonía y Videoconferencia *IP*, tales como: *H.323* y *SIP*. *H.323* es un protocolo que varía en la implementación de cada marca y hace dependiente a la empresa solamente a una marca.

SIP es un estándar definido que garantiza la compatibilidad entre diferentes fabricantes, si son compatibles con *SIP*. Por lo general las Centrales *IP* puras son compatibles con *SIP*, existen teléfonos *SIP* en *hardware* y *software*; los teléfonos *SIP* en *software* se pueden cargar en teléfonos inteligentes o *PDA*.

Se diseñará la red inalámbrica como complemento a la red cableada, en caso de falta de puntos de red o para usuarios móviles. Por medio de la red inalámbrica se dará acceso a los teléfonos inalámbricos *SIP*, celulares con red inalámbrica, *PDA*s con *software SIP*, etc.

²⁴ *PoE* (*Power over Ethernet*) estándar *IEEE 802.3af*

²⁵ Listas de Control de Acceso

3.2.1 REDISEÑO RED CABLEADA

La red cableada es la base sobre la cual se ejecutarán sistemas de voz, datos y video. Actualmente se tienen dos redes separadas una para datos y otra de telefonía, por lo que la administración de dos redes se dificulta mucho para el personal de la empresa.

Al no existir administración remota de los equipos de red y telefonía, el personal de la empresa se tiene que desplazar entre las sucursales y muchas veces entre ciudades para arreglar problemas, que se podrían solucionar remotamente con un programa que administre una sola red convergente.

Al tener una sola red convergente y administrable se disminuirán tiempos de resolución de fallas, así como costos en desplazamientos entre sucursales y en el peor de los casos entre ciudades. Adicionalmente se disminuirá el cableado necesario para la telefonía al necesitar de un solo cable para cada usuario de la red por donde se transmitirán voz, datos y video.

La red cableada se diseñará con:

- 100 *Base TX* para Estaciones de Trabajo
- 1000 *Base T* para Servidores; cumpliendo la norma de cableado estructurado EIA / TIA 568B en todos los puntos de red de la empresa.

Las estaciones de trabajo no generan tanto flujo de información como para tener una red *gigabit* íntegramente; si bien es cierto que se va a utilizar el mismo puerto para telefonía y datos es suficiente el estándar 100 *Base TX*.

Los servidores atienden a muchos usuarios y necesitan puertos 1000 *Base T*. Los servidores se conectarán de forma redundante utilizando dos puertos que manejen balanceo de carga y caminos redundantes; en caso de fallas uno de los dos asumirá todo el tráfico del servidor.

3.2.1.1 Sucursales Quito

3.2.1.1.1 Sucursal Principal

Esta sucursal tiene 40 equipos en la red que al momento se conectan de forma cableada, por lo que se tienen 40 puntos de cableado estructurado. La telefonía *IP* que es parte de este diseño va a utilizar el mismo punto de red que el equipo ya instalado para no incurrir en gastos de nuevo cableado.

Sucursal Principal				
Puertos	Computadores, Telefonía e Impresoras de Red	Access Point	Central Telefónica <i>IP</i>	Servidores
10/100 <i>Base T</i>	40	2	1 x 2	1 x 2
10/100/1000 <i>Base T</i>				2 x 2

Tabla 3-1: Dimensionamiento de *Switches* para la Sucursal Principal

Los servidores, la central telefónica se conectan a los *switches* utilizando dos puertos del *switch* para proporcionar redundancia en caso de fallas y balanceo de carga. En la Tabla 3-1 se detalla 2 x 2 en Servidores, es decir se tienen dos servidores con conexiones redundantes; lo mismo con la central telefónica. Los puertos del *stack* son generalmente los dos últimos puertos *gigabit* del *switch*.

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 <i>Base T</i>	46	10	56
10/100/1000 <i>Base T</i>	4	0	4
<i>Stack</i>	2 (por <i>switch</i>)	0	4

Tabla 3-2: Cálculo de puertos en *switches* para la Sucursal Principal

El porcentaje de crecimiento para el dimensionamiento de los *switches* es 20% que es prudente para el futuro crecimiento. Adicionalmente, se debe tener en cuenta que se deben reservar puertos para administración de las *VLANs*, por ejemplo: la *VLAN* de administración y del *stack* de los *switches*; no se tienen usuarios fijos pero si un puerto reservado para administración.

Los equipos necesarios para la red son especificados en la Tabla 3-3.

Cantidad	Ítem	Características	Puertos
1	Switch	Capa 3, soporte <i>RIP v2</i> , <i>VLANs</i> , <i>QoS</i>	48 puertos 10/100 Base TX, 2 10/100/1000 Base T, 2 puertos stack
1	Switch	Capa 3, soporte <i>RIP v2</i> , <i>VLANs</i> , <i>QoS</i>	24 puertos 10/100 Base TX, 2 10/100/1000 Base T, 2 puertos stack
1	Ruteador	Soporte: <i>QoS</i> , <i>RIP v2</i> , <i>OSPF</i>	1 puerto WAN V.35 y 1 puerto LAN 10/100 Base TX
1	Sistema de Seguridad Unificado	<i>Firewall</i> , <i>IPS</i> , inicia y termina <i>VPN</i> , 40 usuarios	1 puerto WAN 10/100 Base TX y 2 puertos LAN 10/100 Base TX
1	Central Telefónica IP	40 extensiones	2 puertos LAN 10/100 Base TX y 1 puerto WAN 10/100 Base TX

Tabla 3-3: Equipos para rediseño de la Sucursal Principal

Se tienen dos alternativas para la red cableada, éstas difieren en la implementación de la Central Telefónica que se utilice, por ejemplo: 3COM maneja Centrales Telefónicas IP con equipos. En cambio, Cisco implementa Telefonía IP en base a un *IOS* especial, los ruteadores que soportan esta versión de *IOS* son los 2800 o superior.

Las alternativas son:

1. En la Figura 3-1 se muestra la red con una central telefónica, la ventaja que se tiene es manejar separadamente la central telefónica y el ruteador. Si se tiene una falla en el ruteador o la central telefónica no se perderá los dos servicios al mismo tiempo, es decir, no se perderá la conectividad con las sucursales y la telefonía sino sólo el sistema defectuoso.

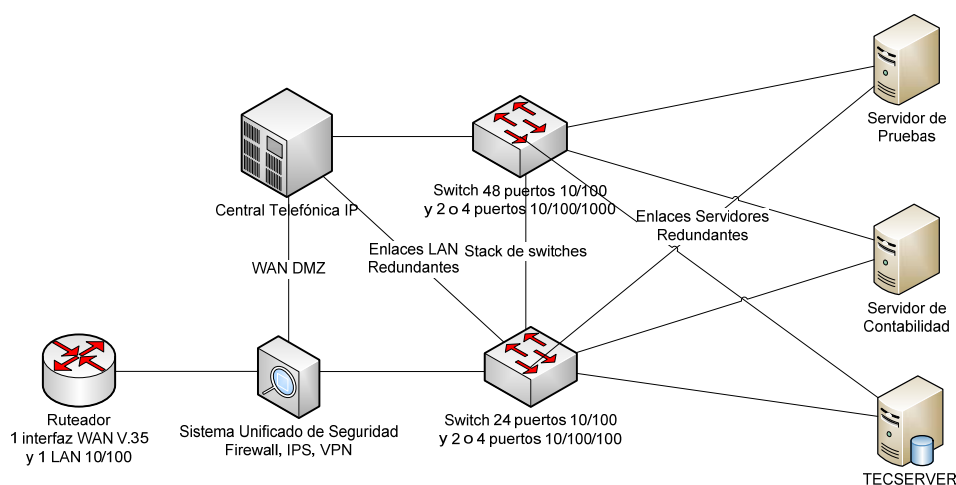


Figura 3-1: Esquema de Red de la Sucursal Principal con Central Telefónica IP

2. La segunda alternativa (Figura 3-2) es con una Central Telefónica *IP Cisco* que se implementa mediante una versión especial de *Cisco IOS* que tiene la funcionalidad de Central *IP*, teniendo un único punto de falla.

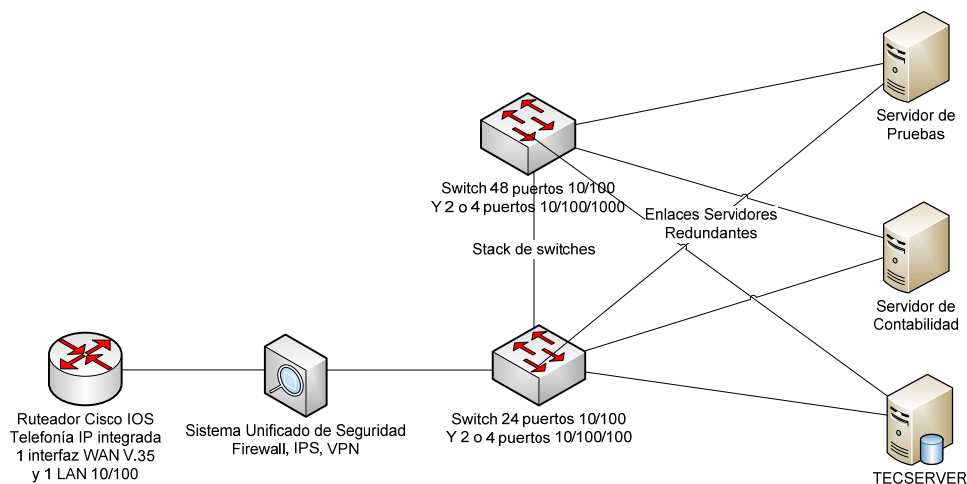


Figura 3-2: Esquema de Red de la Sucursal Principal Central Telefónica *IP Cisco*

Dentro de las dos alternativas, el esquema de los *switches* es el mismo, están conectados por medio de un *stack* favoreciendo su administración; con un solo *stack* se tiene una sola dirección *IP* para administración reduciendo la complejidad de la red. Adicionalmente, se incrementa la tolerancia a fallas por tener redundancia de *switches*, para los equipos críticos tales como:

- Servidor *Tecserver*
- Computadores del Departamento de Ventas
- Computadores de las Cajas
- Computadores de Bodega
- Computadores del Departamento de Crédito

3.2.1.1.2 Sucursal Colón

En la Sucursal Colón de Quito trabajan 17 personas como usuarios de la red, adicionalmente en esta sucursal se tiene el servidor BETA que tiene la base de datos de esta sucursal.

Sucursal Colón				
Puertos	Computadores, Telefonía e Impresoras de Red	Central Telefónica IP	Access Point	Servidores
10/100 Base T	18	2	4	
10/100/1000 Base T				2 x 2

Tabla 3-4: Dimensionamiento en Switches de la Sucursal Colón

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 Base T	24	5	29
10/100/1000 Base T	4	0	4
Stack	2 (por switch)	0	4

Tabla 3-5: Cálculo de Puertos en Switches de la Sucursal Colón

Los equipos necesarios para la red son especificados en la Tabla 3-6.

Cantidad	Ítem	Características	Puertos
2	Switch	Capa 3, soporte RIP v2, VLANs, QoS	24 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T, 2 puertos stack
1	Ruteador	Soporte: QoS, RIP v2, OSPF	1 puerto WAN V.35 y 1 puerto LAN 10/100 Base T
1	Sistema Unificado de Seguridad	Firewall, IPS, inicia y termina VPN, 17 usuarios	1 puerto WAN 10/100 Base T y 2 puertos LAN 10/100 Base T
1	Central Telefónica IP	17 extensiones	2 puertos LAN 10/100 Base T y 1 puerto WAN 10 /100 Base T

Tabla 3-6: Equipos del Rediseño de la Sucursal Colón

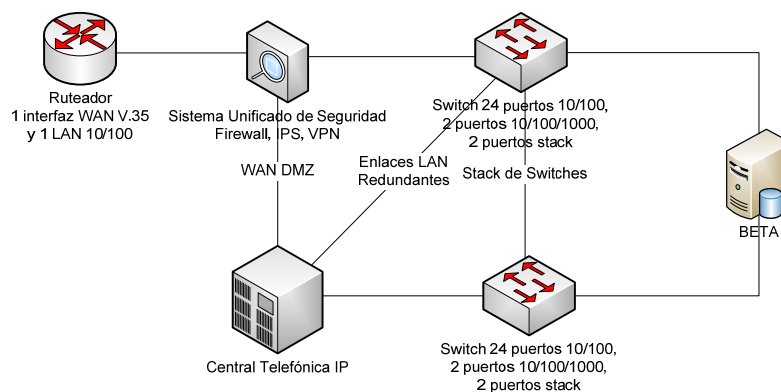


Figura 3-3: Esquema de Red del Rediseño de la Sucursal Colón

Al tener voz, datos y video en una red convergente se debe procurar tener la mayor disponibilidad posible. El *stack* de *switches* es una forma de incrementar la disponibilidad de la red; se citan dos ejemplos:

- En caso de falla de uno de los *switches*, se lo reemplaza, se lo conecta al *stack* y se configura automáticamente el *switch* insertado;

- Al tener dos o más switches en un *stack* no sólo se tiene un único punto de falla, se puede balancear los equipos críticos para cuando exista un fallo en un *switch* los otros equipos de los mismos departamentos sigan conectados al otro *switch*.

Adicionalmente se debe contratar una garantía de reemplazo de equipos en un tiempo máximo de 24 horas, y soporte técnico en las horas de trabajo de la empresa o 24 horas al día, porque la empresa trabaja más de 8 horas.

3.2.1.1.3 Sucursal CST

En la Sucursal CST de Quito trabajan 23 personas; en esta sucursal se tiene un Servidor *Web* que consolida la información de las bases de datos de todas las sucursales a nivel nacional, para las consultas realizadas desde la página *Web* y la *Intranet*.

Para el dimensionamiento de puertos de los *switches* de la sucursal se toman en cuenta los usuarios, equipos de conectividad y centrales telefónicas, detallados en la Tabla 3-7.

Sucursal CST				
Puertos	Computadores, Telefonía e Impresoras de Red	Central Telefónica IP	Access Point	Servidores
10/100 Base T	28	2	2	
10/100/1000 Base T				1 x 2

Tabla 3-7: Dimensionamiento de *Switches* para la Sucursal CST

Se necesita de preferencia dos *switches* de 24 puertos, porque 32 puertos son requeridos sin tomar en cuenta la capacidad de crecimiento futuro. Al tener dos *switches* de 24 puertos en vez de uno de 48 puertos, se agrega redundancia a la red incrementando su disponibilidad.

En la Tabla 3-8 se dimensionan los *switches* de la Sucursal CST teniendo en cuenta una capacidad de crecimiento del 20%.

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 Base T	32	7	39
10/100/1000 Base T	2	0	2
Stack	2 (por switch)	0	4

Tabla 3-8: Cálculo de Puertos en Switches de la Sucursal CST

Después del dimensionamiento, con la reserva de capacidad de crecimiento, se concluye que son suficientes dos *switches* de 24 puertos para los 39 puertos requeridos en el diseño.

Los equipos necesarios para la red son especificados en la Tabla 3-9.

Cantidad	Ítem	Características	Puertos
2	Switch	Capa 3, soporte RIP v2, VLANs, QoS	24 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T y 2 puertos stack
1	Ruteador	Soporte: QoS, RIP v2, OSPF	4 puertos WAN V.35 y 1 puerto LAN 10/100 Base T
1	Sistema Unificado de Seguridad	Firewall, IPS, inicia y termina VPN, 23 usuarios	1 puerto LAN 10/100 Base T y 1 puerto WAN 10/100 Base T
1	Central Telefónica IP	23 extensiones	1 puerto LAN 10/100 Base T

Tabla 3-9: Equipos de Red para Rediseño de la Sucursal CST

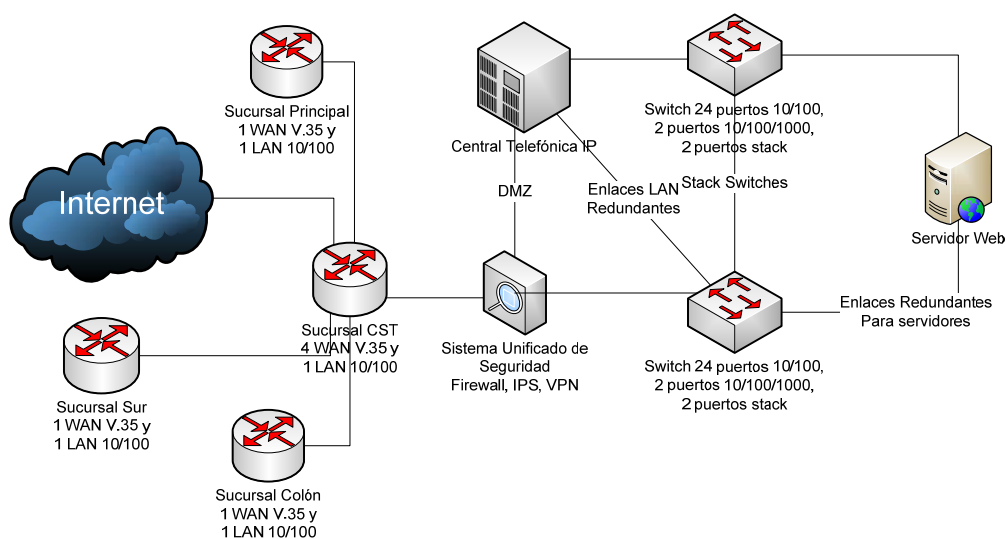


Figura 3-4: Esquema de Red Rediseñada para la Sucursal CST

Por medio de esta sucursal se interconectan las sucursales de Quito utilizando enlaces privados cableados e inalámbricos; el ruteador de esta sucursal tiene cuatro interfaces *WAN* para manejar los tres enlaces con las sucursales y la conexión de *Internet* centralizada para Quito.

3.2.1.1.4 Sucursal Sur

En la Sucursal Sur de Quito trabajan 11 personas, en ella se tienen un servidor llamado OMEGA que tiene la base de datos. Esta sucursal es la más pequeña de Quito y no se va a tener *stack* de *switches* para un número tan reducido de usuarios, con un *switch* es más que suficiente.

Sucursal Sur				
Puertos	Computadores, Telefonía e Impresoras de Red	Central Telefónica IP	Access Point	Servidores
10/100 Base T	12	2	2	
10/100/1000 Base T				1

Tabla 3-10: Dimensionamiento en Switches de la Sucursal Sur de Quito

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 Base T	16	4	20
10/100/1000 Base T	1	0	1

Tabla 3-11: Cálculo de Puertos en Switches de la Sucursal Sur de Quito

Los equipos necesarios para la red son especificados en la Tabla 3-12.

Cantidad	Ítem	Características	Puertos
1	Switch	Capa 3, soporte RIP v2, VLANs, QoS	24 puertos 10/100 Base T y 1 puerto 10/100/1000 Base T
1	Ruteador	Soporte: QoS, RIP v2, OSPF	1 puerto WAN V.35 y 1 puerto LAN 10/100 Base T
1	Sistema Unificado de Seguridad	Firewall, IPS, inicia y termina VPN, DMZ, 11 usuarios	2 puertos LAN 10/100 Base T y 1 puerto WAN 10/100 Base T
1	Central Telefónica IP	11 extensiones	1 puerto LAN 10/100 Base T y 1 puerto WAN 10/100 Base T

Tabla 3-12: Equipos de Red para Rediseñada de la Sucursal Sur de Quito

Todos los *switches* deberán tener una garantía de reemplazo menor o igual a 24 horas en caso de fallas, para no tener períodos largos de indisponibilidad en esta sucursal.

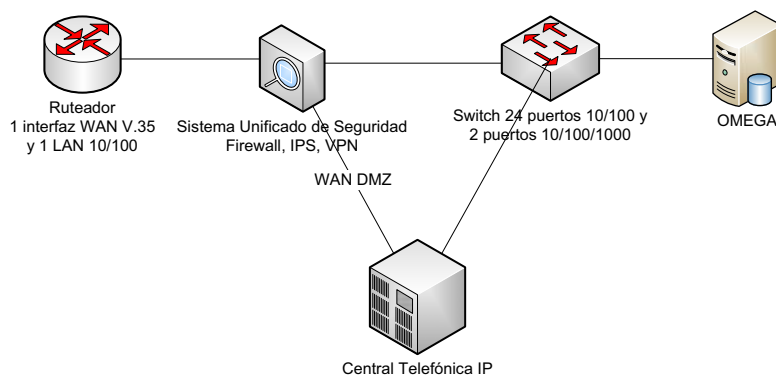


Figura 3-5: Esquema de Red Rediseñada Sucursal Sur de Quito

3.2.1.2 Sucursales Guayaquil

3.2.1.2.1 Sucursal Mayor

En la Sucursal Mayor de Guayaquil trabajan 23 personas, en ésta se tiene un servidor llamado GUAYAQUIL que tiene la base de datos. Al ser esta sucursal la principal de Guayaquil se instalará la conexión a *Internet* y el enlace con la Sucursal Sur.

Sucursal Mayor				
Puertos	Computadores, Telefonía e Impresoras de Red	Central Telefónica IP	Access Point	Servidores
10/100 Base T	24	2	2	
10/100/1000 Base T				1 x 2

Tabla 3-13: Dimensionamiento en *Switches* para la Sucursal Mayor de Guayaquil

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 Base T	28	6	34
10/100/1000 Base T	2	0	2
Stack	2 (por switch)	0	4

Tabla 3-14: Cálculo de Puertos en *Switches* de la Sucursal Mayor de Guayaquil

Como se puede observar en esta sucursal se manejará un *stack* de *switches* para incrementar la disponibilidad y redundancia en caso de fallas.

Los equipos necesarios para la red son especificados en la Tabla 3-15.

Cantidad	Ítem	Características	Puertos
2	Switch	Capa 3, que soporte <i>RIP v2</i> , <i>VLANs</i> , <i>QoS</i>	24 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T y 2 puertos <i>stack</i>
1	Ruteador	Soporte: <i>QoS</i> , <i>RIP v2</i> , <i>OSPF</i>	2 puertos WAN V.35 y 1 puerto LAN 10/100 Base T
1	Sistema Unificado de Seguridad	<i>Firewall</i> , <i>IPS</i> , inicia y termina <i>VPN</i> , <i>DMZ</i> , 22 usuarios	2 puertos LAN 10/100 Base T y 1 puerto WAN 10/100 Base T
1	Central Telefónica IP	22 extensiones	2 puertos LAN 10/100 Base T y 1 puerto WAN 10/100 Base T

Tabla 3-15: Equipos de Red Rediseñada para la Sucursal Mayor de Guayaquil

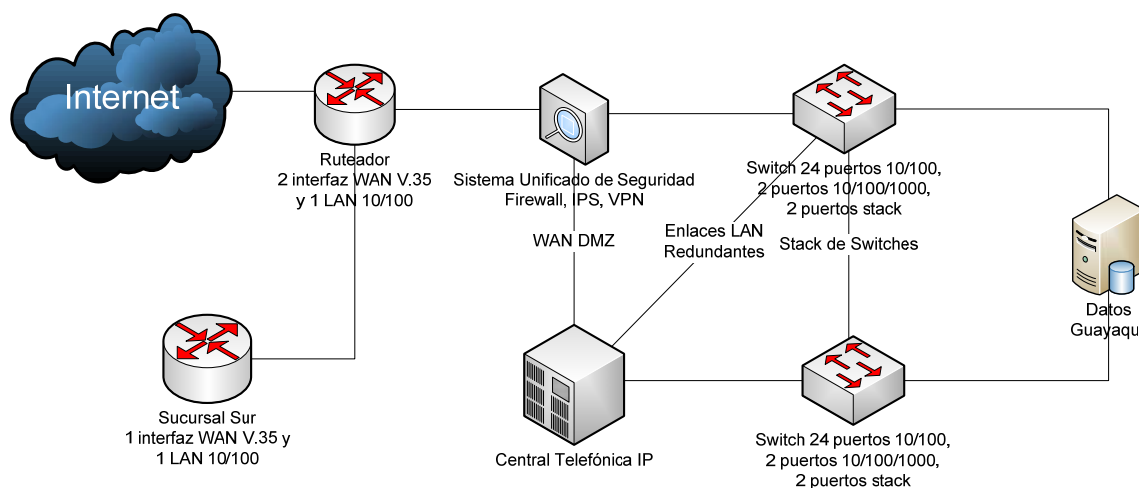


Figura 3-6: Esquema de Red Rediseñada para la Sucursal Mayor de Guayaquil

3.2.1.2.2 Sucursal Sur

En la Sucursal Sur de Guayaquil trabajan 9 personas, en ésta se tiene un servidor llamado *SIGMA* que tiene la base de datos. Igualmente que la Sucursal Sur de Quito, es muy pequeña para implementar un *stack* de *switches*, sólo se ubicará un *switch* de 24 puertos.

Sucursal Sur de Guayaquil				
Puertos	Computadores, Telefonía e Impresoras de Red	Central Telefónica IP	Access Point	Servidores
10/100 Base T	10	2	1	
10/100/1000 Base T				1

Tabla 3-16: Dimensionamiento en Switches para la Sucursal Sur de Guayaquil

Puertos	# puertos necesarios	% 20 de crecimiento	Total
10/100 Base T	13	3	16
10/100/1000 Base T	1	0	1

Tabla 3-17: Cálculo de Puertos en Switches para la Sucursal Sur de Guayaquil

Los equipos necesarios para la red son especificados en la Tabla 3-18.

Cantidad	Ítem	Características	Puertos
1	Switch	Capa 3, soporte RIP v2, VLANs, QoS	24 puertos 10/100 Base T y 1 puerto 10/100/1000 Base T
1	Ruteador	Soporte: QoS, RIP v2, OSPF	1 puerto WAN V.35 y 1 puerto LAN 10/100 Base T
1	Sistema Unificado de Seguridad	Firewall, IPS, inicia y termina VPN, DMZ, 9 usuarios	2 puertos LAN 10/100 Base T y 1 puertos WAN 10/100 Base T
1	Central Telefónica IP	9 extensiones	1 puerto LAN 10/100 Base T y 1 puerto WAN 10/100 Base T

Tabla 3-18: Equipos de Red Rediseñada para la Sucursal Sur de Guayaquil

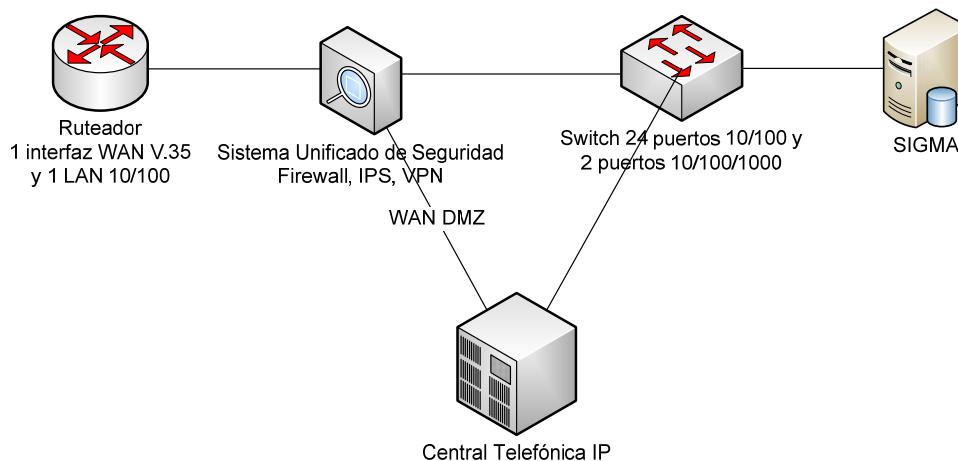


Figura 3-7: Esquema de Red Rediseñada para la Sucursal Sur de Guayaquil

Todos los switches deberán tener una garantía de reemplazo menor o igual a 24 horas en caso de fallas, para no tener períodos largos de falta de disponibilidad en esta sucursal.

3.2.2 RED INALÁMBRICA

Las redes inalámbricas brindan movilidad a los usuarios y sirven como complemento a la red cableada cuando se tiene falta de puntos de red en una oficina. Los usuarios inalámbricos tendrán cobertura en todas las sucursales, con sólo ingresar su nombre de usuario y contraseña accederán a la red.

La red inalámbrica brindará los mismos servicios que la red cableada; para esto se tomarán en cuenta sistemas de seguridad con autenticación de usuarios, encriptación de información, etc. La seguridad de la red inalámbrica cumplirá los mismos estándares que la red cableada, más aquellos propios de redes inalámbricas seguras.

Los clientes inalámbricos que son empleados de la empresa estarán en la misma *VLAN* que los demás usuarios que se conectan de forma cableada a la red para tener acceso a los servidores, a la Aplicación *Global Commerce*; también se tienen acceso a la *VLAN* de Telefonía *IP*, para sincronizar los teléfonos *SIP* instalados en sus celulares, *PDA*s, o computadores.

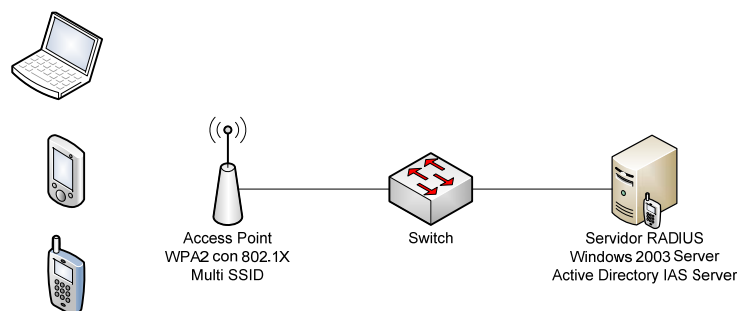


Figura 3-8: Esquema de Red Inalámbrica

El esquema de seguridad inalámbrica a implementarse es 802.11i (*WPA2*) que es el más robusto actualmente, porque *WEP* y *WPA* fueron criptoanalizados, siendo por estas razones no aconsejables para una empresa estos esquemas de seguridad inalámbrica.

La autenticación de los empleados se realiza mediante el servicio *IAS* (*Internet Authentication Server*) que trabajará como Servidor *RADIUS*; el manejo de usuarios y contraseñas se realizará con el dominio que está integrado con *Active Directory* de *Microsoft*.

El esquema de seguridad que se va a manejar es *PEAP-EAP-MS-CHAPv2*, que no necesita de certificados digitales instalados en el cliente y sólo necesita de un nombre de usuario y su contraseña para la autenticación; en el servidor si se debe instalar un certificado digital para su autenticación.

Para los clientes se ha pensado dar servicio de *Internet* Inalámbrico teniendo una *VLAN* aislada de la red, para que los clientes puedan contactarse con su oficina para consultar lo que tienen que comprar o retirar en Tecnomega, conversar con sus clientes por medio de Mensajería Instantánea o *VoIP*, etc.

Los clientes que deseen acceder a la red inalámbrica deben solicitar la clave al departamento de sistemas. La seguridad a implementar para los clientes será *WPA2* compatible para atrás con *WPA* con una clave compartida para aumentar su compatibilidad; para limitar el uso no autorizado de este servicio se va a restringir a las direcciones *MAC* registradas para poder ingresar.

Esta *VLAN* solo tendrá acceso a *Internet* y deberá ser lo suficientemente segura para que no permita el acceso a la red de la empresa. Los equipos que se incorporarán para la seguridad deben tener características especiales para aislar totalmente ciertas *VLANs* para clientes y para los empleados.

Los *access points* deben tener las siguientes características:

- Estándar 802.11g
- Antenas intercambiables
- Soporte *SNMP*, *QoS*, *PoE*, *Multi SSID*, *VLANs*, *WPA2 Enterprise*

Los *access point* necesarios son:

Sucursal	Cantidad	Equipo	Características
Principal (Quito)	2	<i>Access Point</i>	1 puerto LAN 10/100 Base T
Colón (Quito)	4	<i>Access Point</i>	1 puerto LAN 10/100 Base T
CST (Quito)	2	<i>Access Point</i>	1 puerto LAN 10/100 Base T
Sur (Quito)	2	<i>Access Point</i>	1 puerto LAN 10/100 Base T
Mayor (Guayaquil)	2	<i>Access Point</i>	1 puerto LAN 10/100 Base T
Sur (Guayaquil)	1	<i>Access Point</i>	1 puerto LAN 10/100 Base T
TOTAL	13		

Tabla 3-19: Número de *Access Points* por Sucursal

En total se necesitan trece *access points* para brindar cobertura inalámbrica a todas las sucursales de Tecnomega en el país; éstos deberán cumplir con todas las características antes descritas, para facilitar su administración mediante *SNMP*. Por otro lado, se facilita su instalación con la característica de *PoE* porque algunos *access points* se quieren instalar en el techo o en las paredes de las sucursales.

El estándar de *PoE* (802.3af) permite brindar energía *DC* por el mismo cable de datos. El beneficio es poder integrar dispositivos a la red *LAN* existente, sin tener que realizar un nuevo cableado eléctrico al no disponer de un punto eléctrico al momento de la instalación del equipo.

Para el rediseño de la red inalámbrica se ha tomado en cuenta pruebas de campo realizadas en cada una de las sucursales, donde se detallan las redes inalámbricas existentes en el ambiente. Mediante estas pruebas se determinará los canales disponibles para la configuración de los equipos.

Al no contar al momento de las pruebas con equipos de características y marca, que se proponen en este proyecto no se realizó un *site survey* activo para verificar la cobertura lograda, por lo que se recomienda realizar este *site survey* para garantizar la cobertura en las oficinas de la empresa.

La distribución planteada de los equipos inalámbricos se la definió mediante los *access points* instalados y la elección de lugares estratégicos según los planos de las sucursales.

3.2.2.1 Sucursales de Quito

3.2.2.1.1 Sucursal Principal

La Sucursal Principal en el primer piso tiene el área de atención al cliente, donde están los vendedores, la bodega, las cajas, el personal de crédito, la división de importaciones y la Gerencia General; en el segundo piso están oficinas de: la Gerencia de Ventas, el Departamento de Sistemas y de Contabilidad; en el subsuelo se encuentra un cuarto de telecomunicaciones donde está ubicado el servidor principal y otros equipos de conectividad.

La red inalámbrica se va a diseñar para dar acceso a *Internet* a los clientes y a los empleados de la empresa; se necesita cubrir toda el área de la sucursal excepto el subsuelo porque se tienen accesos esporádicos a este lugar.

A continuación se diseña la ubicación idónea de los puntos inalámbricos, el número de puntos que se necesitan y especificaciones de seguridad para cumplir con las Políticas de Seguridad.

En el plano del primer piso se puede determinar el lugar idóneo para la ubicación del punto inalámbrico, que no sea muy inseguro su acceso físico; se lo instalará en la pared que está detrás de la recepción, así se logra tener una intensidad casi homogénea en toda el área del primer piso. Para mejorar la señal se sugiere instalar antena(s) omnidireccionales de alta ganancia entre 5 *dBi* y 7 *dBi* según el equipo inalámbrico utilice una o dos antenas.

El equipo inalámbrico a instalarse es un *access point* que cumpla con el estándar 802.11g, ya que es el más utilizado y se busca la mayor compatibilidad con los equipos inalámbricos actuales.

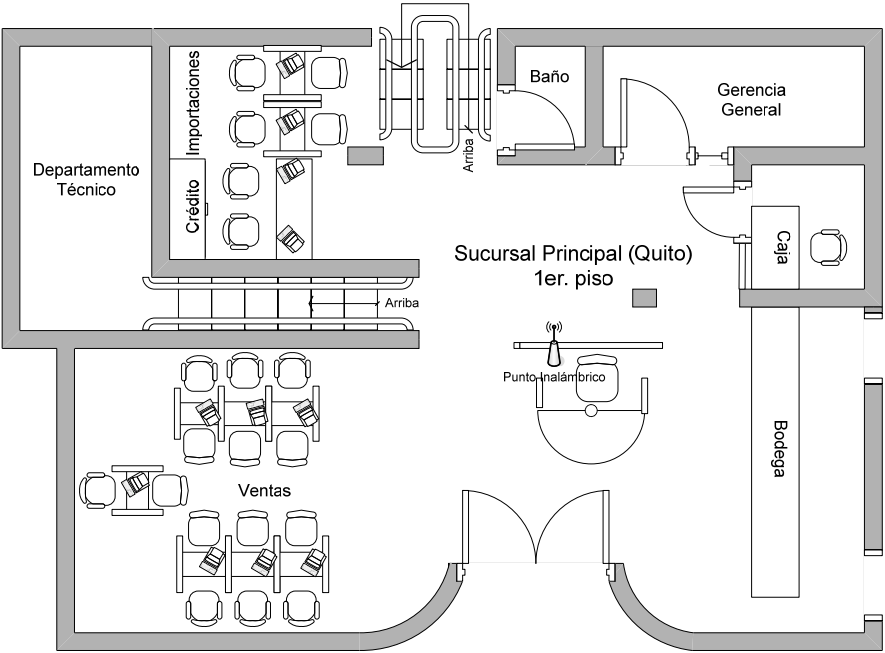


Figura 3-9: Plano del Primer Piso de la Sucursal Principal

En la segunda planta de esta sucursal, se ubicará un punto inalámbrico para que funcione como repetidor del *access point* del primer piso, logrando ampliar la cobertura de la red inalámbrica de forma transparente para el usuario. Cuando los *access points* trabajan como repetidores funcionan el *root* (principal) y el repetidor, en el mismo canal.

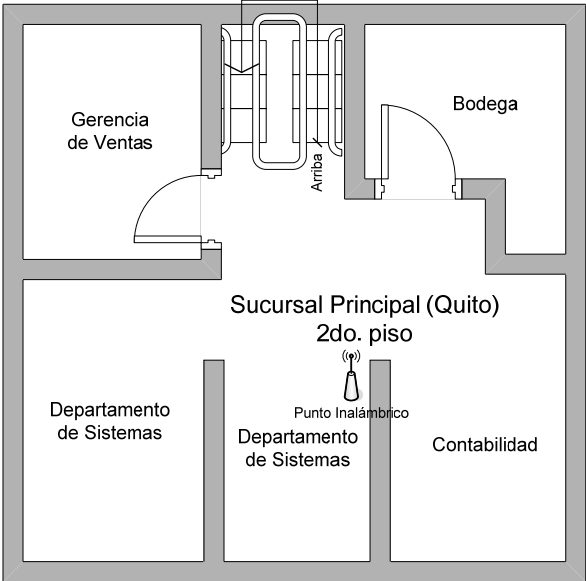


Figura 3-10: Plano del Segundo Piso de la Sucursal Principal

El *access point* del segundo piso debe ser estratégicamente ubicado donde se muestra en la Figura 3-10, colocado sobre la pared. En este punto, el *access point* tiene buena cobertura en especial para la Gerencia de Ventas y el Departamento de Sistemas donde pueden existir clientes que tengan reuniones con los empleados de estos departamentos.

Site Survey Pasivo Sucursal Principal

SSID	Señal ²⁶	Canal	Tipo de Red	Tipo de Radio	Autenticación	Cifrado
FC	0 %	6	Infraestructura	802.11g	Abierta	WEP
Codeu	17 %	11	Infraestructura	802.11g	WPA-Personal	TKIP
Cybercell01	0 %	8	Infraestructura	802.11g	Abierta	WEP

Tabla 3-20: Site Survey Sucursal Principal

Configuración de los Equipos Inalámbricos

- SSID: principal VLAN empleados
- SSID: cli_principal VLAN clientes
- Equipo1: Modo *Access Point* (normal)
- Equipo2: Modo Repetidor
- Antenas de Expansión de: 5 dBi o más.
- Canal: 1
- Seguridad Inalámbrica: *WPA2 Enterprise* con 802.1X, con esquema de seguridad *PEAP-EAP-MS-CHAPv2*

²⁶ El % de señal, es el pico en el área de las oficinas de la empresa. Se debe tener en cuenta que el rango es de – 45 a – 95 dBm que corresponden a 100 al 0% respectivamente. Señal alta de – 45 a -65 dBm (100 a 60 %), señal buena – 66 a – 85 dBm (58 a 20 %) y señal baja – 86 a – 95 dBm (18 a 0 %)

3.2.2.1.2 Sucursal Colón

La sucursal Colón fue recientemente construida y tiene dos pisos. El primer piso se encuentra el área de atención al cliente que es un rectángulo grande sin paredes que interfieran la señal inalámbrica; por su gran tamaño se ubicará dos *access points* trabajando el primero como *root* y el segundo como repetidor para dar cobertura inalámbrica en toda la planta. Estos equipos serán instalados en el techo tal como se muestra en la Figura 3-11.

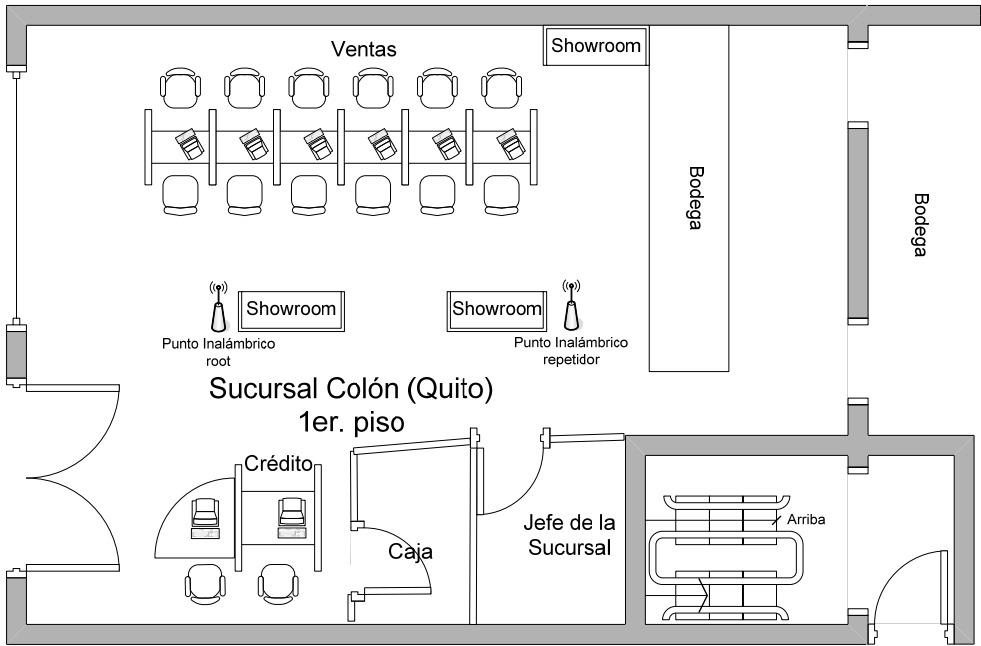


Figura 3-11: Plano del Primer Piso de la Sucursal Colón

Con esta configuración de repetidores se amplía la cobertura de la red inalámbrica y no se saturan los canales disponibles al utilizar el mismo canal en los dos *access points*.

Site Survey Pasivo Sucursal Colón

SSID	Canal	Tipo de Red	Tipo de Radio	Autenticación	Cifrado
NETGEAR	11	Infraestructura	802.11g	WPA-Personal	TKIP

Tabla 3-21: Site Survey Sucursal Colón

Configuración de los Equipos Inalámbricos en el Primer Piso

- SSID: colon VLAN empleados
- SSID: cli_colon VLAN clientes
- Equipo1 (ROOT): Modo *Access Point* (normal)
- Equipo2 (REPETIDOR): Modo Repetidor
- Antenas de Expansión de: 5 dBi o más.
- Canal: 1
- Seguridad Inalámbrica: WPA2 Enterprise con 802.1 X, con autenticación PEAP-EAP-MS-CHAPv2

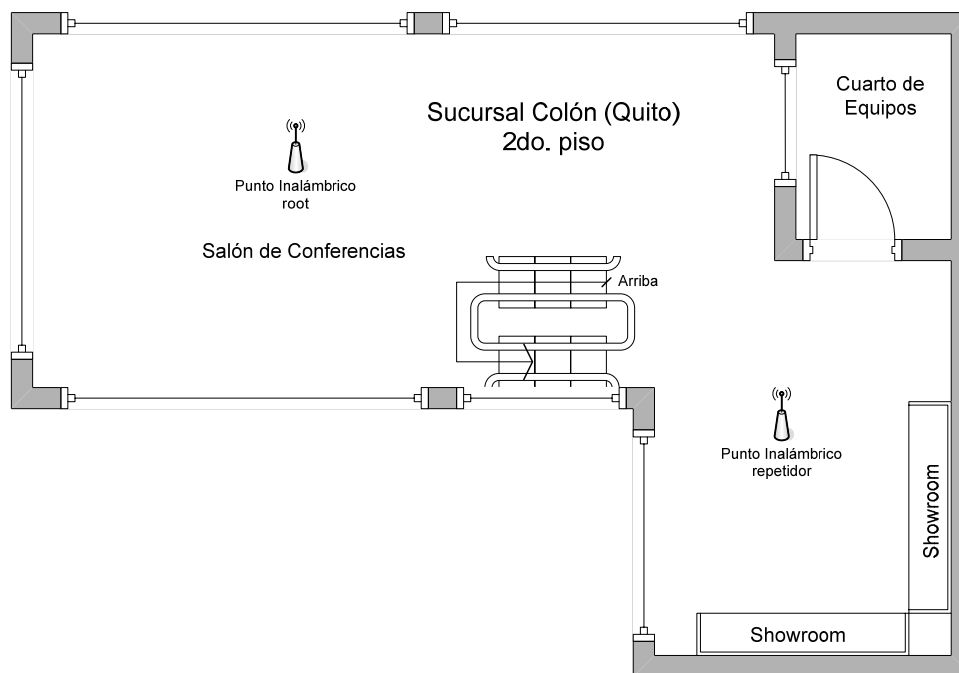


Figura 3-12: Plano del Segundo Piso de la Sucursal Colón

En el segundo piso de esta sucursal se utilizarán dos *access points* en modo repetidor, en otro canal con un SSID diferente al del primer piso, para no interferir con la red inalámbrica del primer piso. Al utilizar otro canal y otro SSID se divide la red, incrementando los usuarios inalámbricos simultáneos que puede soportar y el rendimiento cuando existan muchos clientes inalámbricos en el auditorio (Salón de Conferencias).

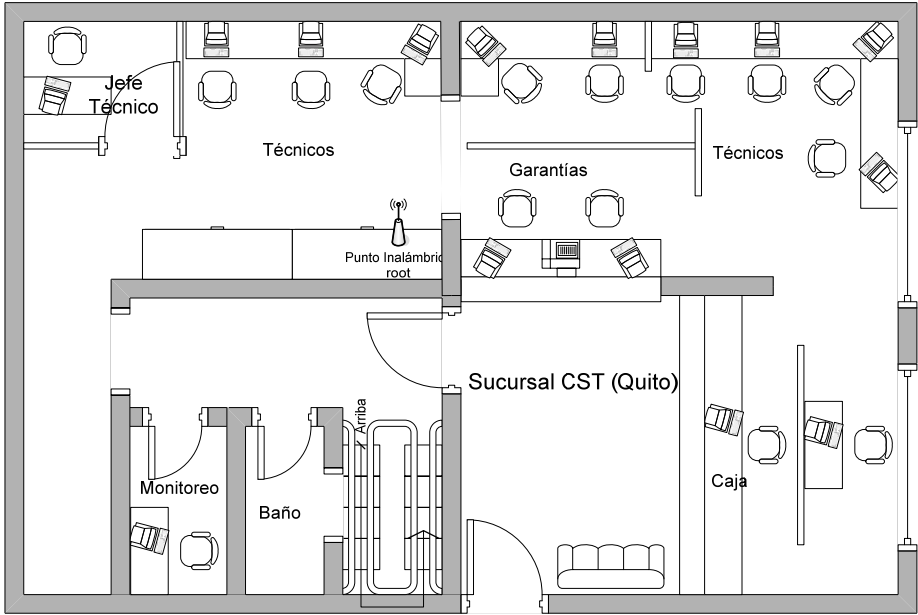


Figura 3-13: Plano del Primer Piso de la Sucursal CST

En el segundo piso se instalará un *access point* en modo Repetidor, tal como se muestra en la Figura 3-14. Este punto tiene buena cobertura inalámbrica al estar ubicado casi en el punto central en esta planta.

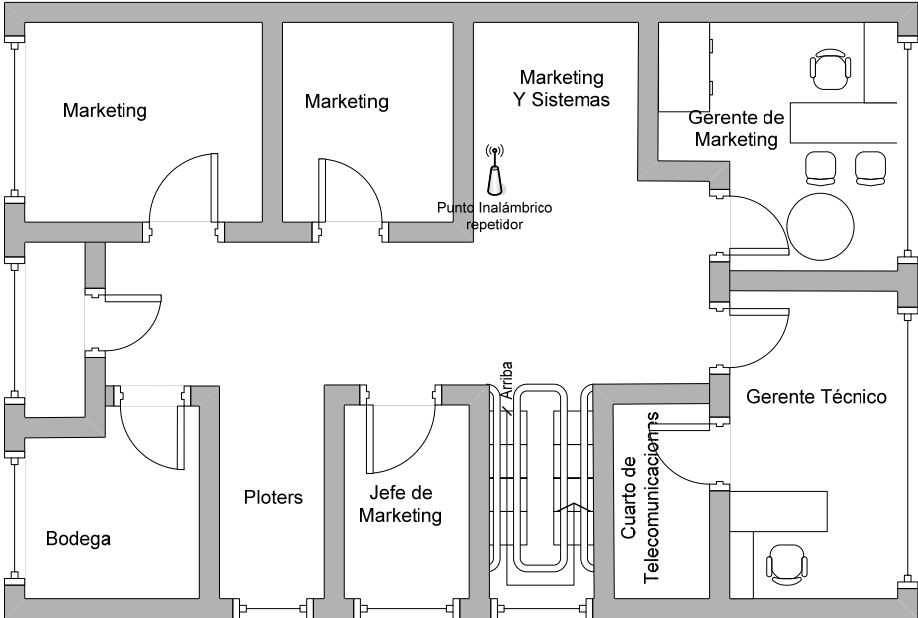


Figura 3-14: Plano del Segundo Piso de la Sucursal CST

En la primera planta se ubicará un punto inalámbrico, colocándolo donde se indica en la Figura 3-15 se obtendrá cobertura en toda la primera planta. Para mejorar la señal inalámbrica y la cobertura se utilizará antenas de expansión.

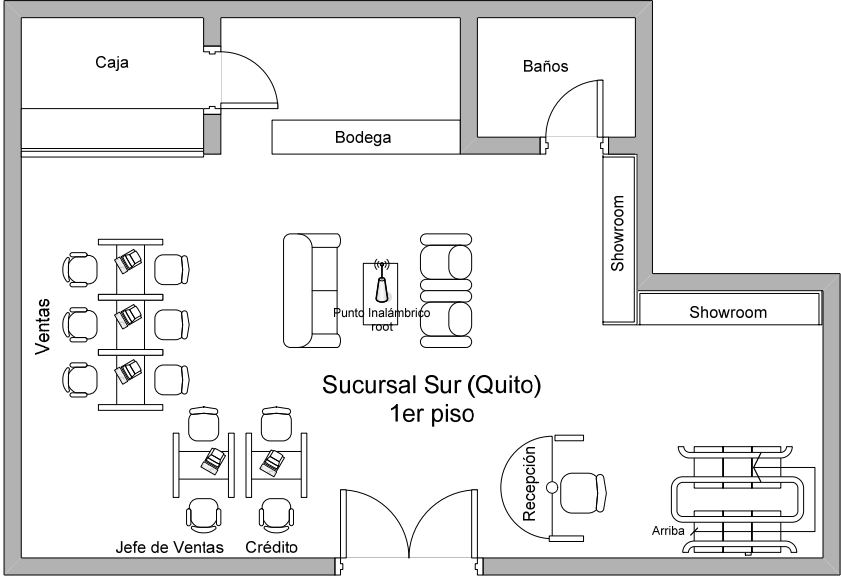


Figura 3-15: Plano del Primer Piso de la Sucursal Sur de Quito

En el segundo piso de la Sucursal Sur se ubicará el punto inalámbrico en el techo como se indica en la Figura 3-16, esta ubicación es central para todas las oficinas de la planta. No se ha ubicado el punto inalámbrico en la pared del auditorio porque es un área con alto tráfico de personas y puede ser susceptible de manipulación, ocasionando una conexión intermitente.

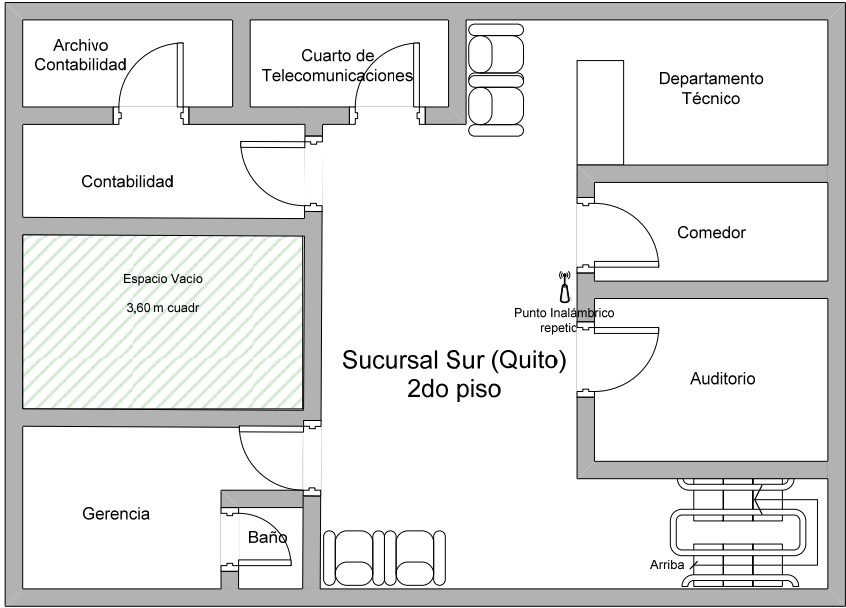


Figura 3-16: Plano del Segundo Piso de la Sucursal Sur de Quito

En estos casos, en los que se tienen oficinas grandes sin divisiones se puede instalar los puntos inalámbricos en el techo, ubicándolos en el centro de la oficina para lograr una cobertura uniforme en todas las direcciones.

En la primera planta se tiene el área de Ventas, Caja, Departamento Técnico; en el segundo piso se tienen la parte Administrativa, Mercadeo, Contabilidad, Departamento Técnico y una sala de reuniones. Se instalarán dos *access point* uno en el primer piso (*ROOT*) y otro en el segundo piso (*REPETIDOR*).

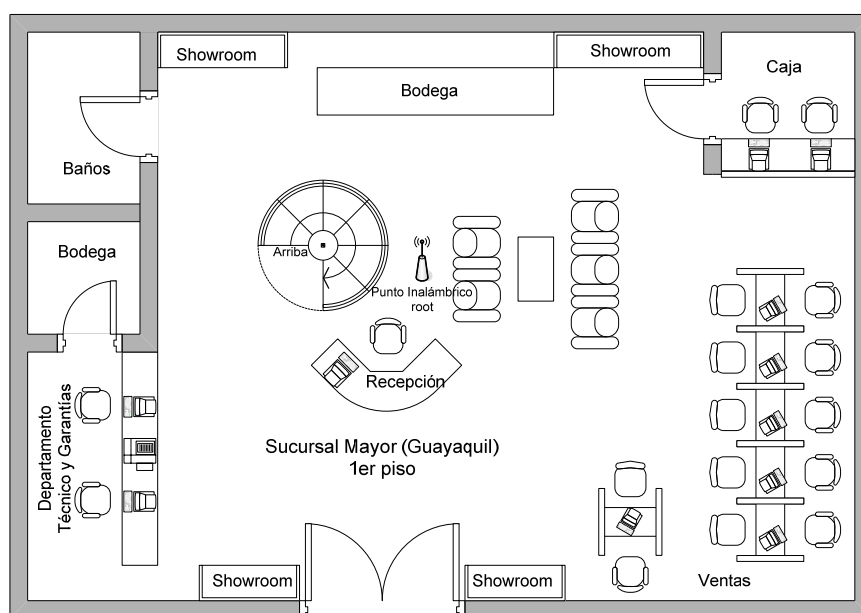


Figura 3-17: Plano del Primer Piso de la Sucursal Mayor de Guayaquil

La ubicación del punto inalámbrico en la primera planta es estratégica, ya que se encuentra en la mitad de la oficina en un lugar inaccesible. Para tener una buena señal y mejorar la cobertura se pueden cambiar las antenas por unas de mayor ganancia.

En segunda planta se instalará el *access point* en el techo, tal como se observa en la Figura 3 - 18 para tener una buena señal y cobertura en todas las direcciones. Esta ubicación es excelente porque está junto a la sala de espera del segundo piso, y próximo al salón de reuniones y al cuarto de telecomunicaciones.

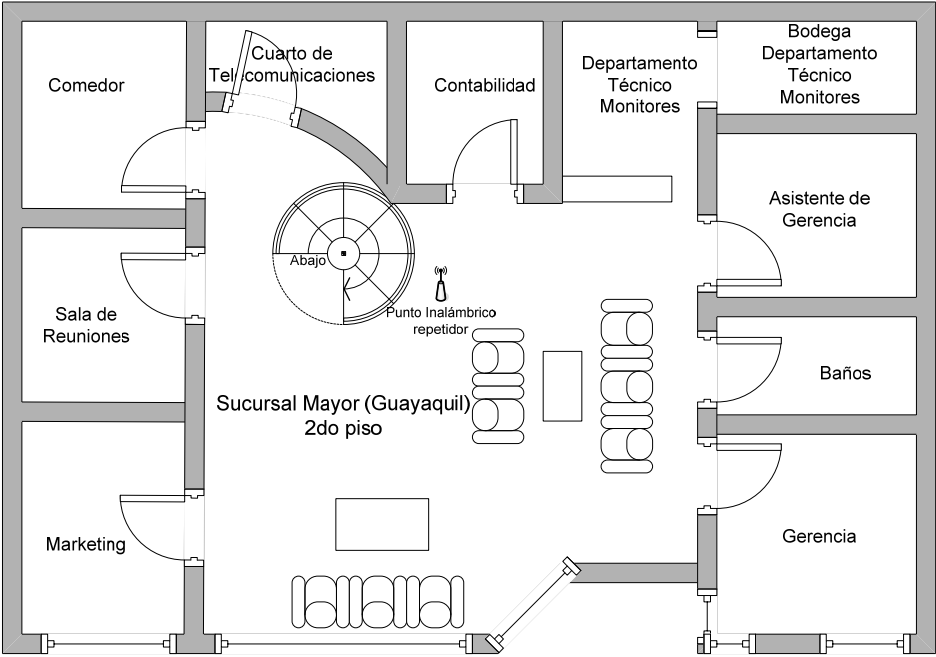


Figura 3-18: Plano del Segundo Piso de la Sucursal Mayor de Guayaquil

Por medio de esta configuración de repetidor se unificará la red y sólo se utilizará un solo canal de frecuencia, lo cual es importante porque en la zona existen un sinnúmero de redes inalámbricas y las frecuencias son escasas. Adicionalmente se logrará una cobertura uniforme en las dos plantas y los usuarios móviles no notarán el cambio al otro *access point* en el caso que se desplacen del primero al segundo piso o viceversa.

Site Survey Pasivo Sucursal Mayor

SSID	Canal	Tipo de Red	Tipo de Radio	Autenticación	Cifrado
linksys	3	Infraestructura	802.11n	WPA2-Personal	CCMP
default	6	Infraestructura	802.11g	Abierta	Ninguna
demo	6	Infraestructura	802.11b	Abierta	Ninguna

Tabla 3-24: Site Survey Sucursal Mayor

Configuración de los Equipos Inalámbricos

- *SSID*: mayor VLAN empleados
- *SSID*: cli_mayor VLAN clientes
- Equipo (*ROOT*): Modo *Access Point* (normal)
- Equipo (*REPETIDOR*): Modo Repetidor
- Antenas de Expansión de: 5 *dBi* o más
- Canal: 11
- Seguridad Inalámbrica: *WPA2 Enterprise* con 802.1X, con autenticación *PEAP-EAP-MS-CHAPv2*.

3.2.2.2 Sucursal Sur

La Sucursal Sur de Guayaquil es la sucursal más pequeña de la empresa, solo cuenta con un piso de oficinas. La oficina es relativamente abierta pero tiene algunas divisiones a los lados para separar espacios, como: Caja, Gerencia, Sala de Reuniones, etc.

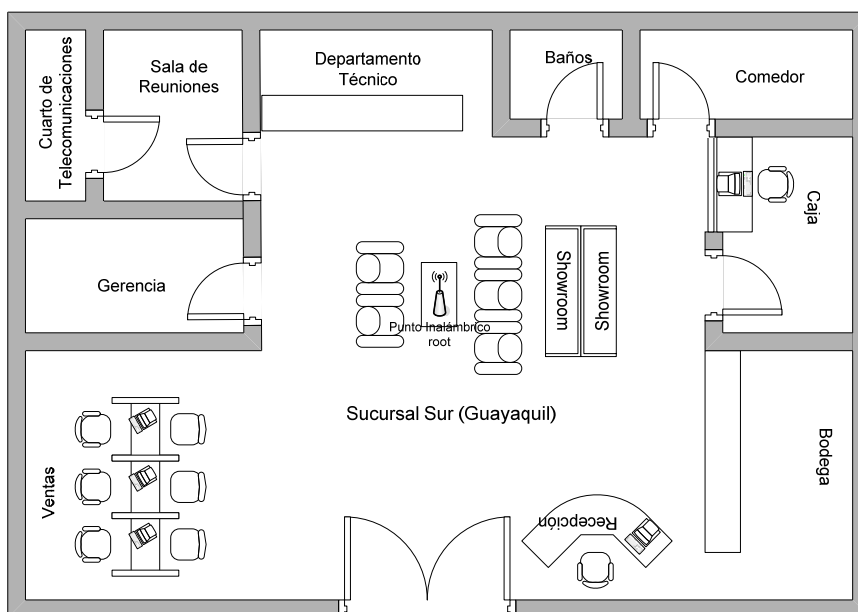


Figura 3-19: Plano de la Sucursal Sur de Guayaquil

3.3 SEGMENTACIÓN DE LA RED POR MEDIO DE VLANs

El diseño de las VLANs tiene que basarse en el tipo de flujo de tráfico en la red. Existe un sistema que administra todas las actividades de la empresa, llamado *Global Commerce* que es utilizado por todos los departamentos. Por esto es algo óptimo realizar la segmentación de VLANs por departamentos.

El uso de VLANs puede ser muy útil pero a la vez puede ser muy perjudicial al rendimiento de la red si no se la diseña correctamente, según la forma de tráfico que tenga la red. La segmentación en VLANs puede ayudar para la administración, seguridad, y el rendimiento de la red, siempre y cuando estén bien diseñadas.

Existen dos tipos de tráfico en redes empresariales, que son 80 – 20 (80% del tráfico se queda en la VLAN y el 20% sale de la ella), éste es el esquema óptimo para el diseño de VLANs; por otro lado se tiene el tráfico 20 – 80 (20% del tráfico se queda en la VLAN y el 80% sale de la ella). En este segundo caso se tiene problema con el diseño de las VLANs porque el mayor flujo de tráfico sale de la VLAN y disminuye el rendimiento de la red, entorpeciendo la VLAN en el tráfico normal de la red.

El flujo de tráfico, si se tienen los servidores en la misma VLAN y los usuarios de la aplicación *Global Commerce* sería 80% dentro de la VLAN y 20% para afuera de la VLAN; este caso cae en la tendencia de centralizar los servicios en las empresas que se tiene actualmente.

En cambio si se diseñaría la segmentación de VLANs por departamentos de la empresa, todos tendrían que trabajar, hacer consultas y manejar el sistema *Global Commerce*, teniendo un tráfico del esquema 20 – 80%, con un rendimiento no deseado, excesivo procesamiento de los *switches* y ruteadores que interconectan las VLANs de la empresa.

Se concluye que el diseño de las *VLANs* debe ser el siguiente:

- *VLANs* necesarias para la administración de los equipos de conectividad:
 - Una *VLAN* de administración de la red
 - Una *VLAN* para administración del *stack* de *switches* que es recomendada por los fabricantes de los equipos.
- Una *VLAN* recomendada por los fabricantes para Telefonía *IP*,
- Una *VLAN* de los clientes inalámbricos que no son empleados, y;
- Una *VLAN* para los empleados.

Se crearán las siguientes *VLANs*:

- Administración
- *Stack*
- Empleados
- Clientes
- Telefonía *IP*

Estas *VLANs* estarán presentes en todas las sucursales de la empresa, por lo que se entrará al diseño del direccionamiento *IP* de cada sucursal según las *VLANs* creadas. El direccionamiento *IP* utilizando en las sucursales pertenece a redes clase C privadas con la dirección de red 192.168.X.0, donde X es el número de la sucursal. En la Tabla 3-26 se determina la asignación de números a las sucursales.

Sucursal	Ciudad	Número	Dirección de Red
Principal	Quito	1	192.168.1.0
Colón	Quito	2	192.168.2.0
CST	Quito	3	192.168.3.0
Sur	Quito	4	192.168.4.0
Mayor	Guayaquil	5	192.168.5.0
Sur	Guayaquil	6	192.168.6.0

Tabla 3-26: Número de las Sucursales para el Direccionamiento *IP*

3.3.1 SUCURSALES DE QUITO

3.3.1.1 Sucursal Principal

La Sucursal Principal de Quito tiene asignada la dirección de red 192.168.1.0. Para la segmentación en *VLANS* se realizará el diseño con Subredes y *VLSM*, y se escogerá la opción que sea viable según la cantidad de direcciones *IP* necesarias en cada subred.

3.3.1.1.1 Diseño con subredes

Dirección de Red: 192.168.1.0

Se necesitan 5 subredes:

- Administración
- *Stack*
- Empleados
- Telefonía *IP*
- Clientes (Inalámbrico)

$$192.168.1.00000000$$

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.1.00000000



Red
Host

$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

Bajo el esquema de subredes no se puede obtener la subred de Telefonía de más de 30 *host*; con este esquema no se podrá manejar todas las extensiones de la sucursal y peor tener una capacidad de crecimiento si se incrementa el número de empleados.

3.3.1.1.2 Diseño con VLSM

El diseño de las subredes con VLSM optimiza las direcciones IP y se consigue un espacio de direcciones IP más que suficiente para Telefonía IP.

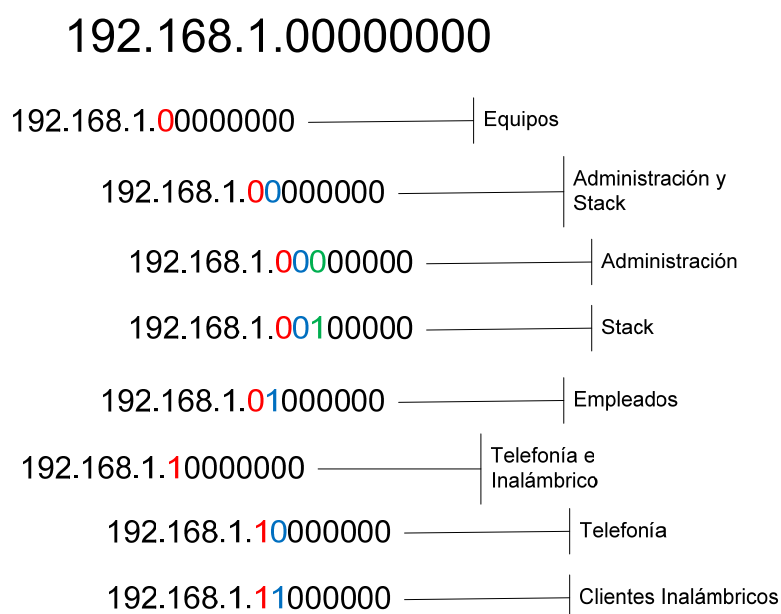


Figura 3-20: Direccionamiento IP Sucursal Principal

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.1.0	255.255.255.224	30
Stack	192.168.1.32	255.255.255.224	30
Empleados	192.168.1.64	255.255.255.192	62
Telefonía	192.168.1.128	255.255.255.192	62
Inalámbrico	192.168.1.192	255.255.255.192	62

Tabla 3-27: VLANs Sucursal Principal

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	30	4	26
Stack	30	1	29
Empleados	62	45	17
Telefonía	62	39	23
Inalámbrico	62	10	52

Tabla 3-28: Host por VLAN Sucursal Principal

El direccionamiento IP cumple con el número de direcciones necesarias para los *host* en cada una de las VLANs y se tiene una capacidad de crecimiento.

3.3.1.2 Sucursal Colón

La Sucursal Colón de Quito tiene asignada la dirección de red 192.168.2.0. Para la segmentación en VLANs se realizará el diseño con Subredes y VLSM, y se escogerá la opción que sea viable según la cantidad de direcciones IP necesarias en cada subred.

3.3.1.2.1 Diseño por Subredes

Dirección de Red: 192.168.2.0

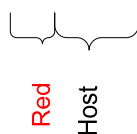
Se necesitan 5 subredes:

- Administración
- Stack
- Empleados
- Telefonía IP
- Clientes (Inalámbrico)

192.168.2.00000000

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.2.00000000



$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

En la Sucursal Colón se podría aplicar este esquema sin problema, con el limitante, si crece el número de empleados se podría tener hasta 30 extensiones en la VLAN de telefonía IP.

3.3.1.2.2 Diseño por VLSM

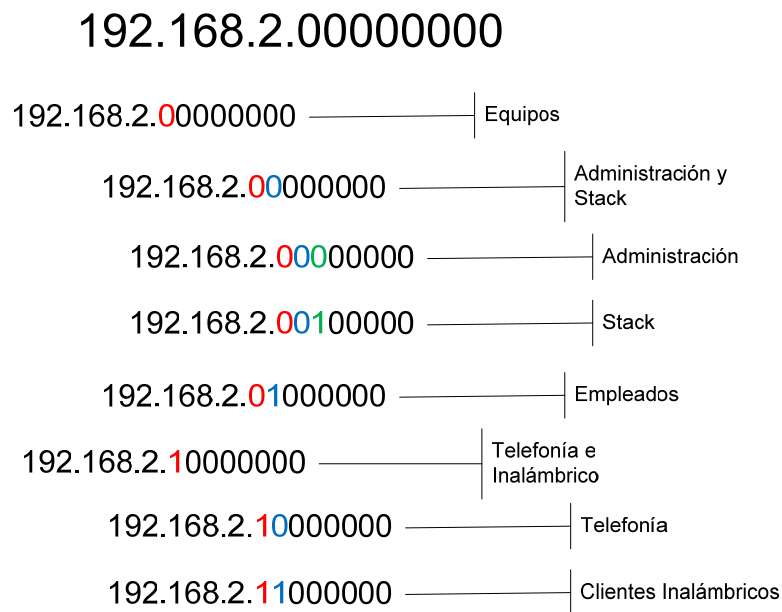


Figura 3-21: Direccionamiento IP Sucursal Colón

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.2.0	255.255.255.224	30
Stack ²⁷	192.168.2.32	255.255.255.224	30
Empleados	192.168.2.64	255.255.255.192	62
Telefonía	192.168.2.128	255.255.255.192	62
Inalámbrico	192.168.2.192	255.255.255.192	62

Tabla 3-29: VLANs Sucursal Colón

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	30	3	27
Stack	30	1	29
Empleados	62	22	42
Telefonía	62	17	45
Inalámbrico	62	10	52

Tabla 3-30: Host por VLAN Sucursal Colón

El esquema de direccionamiento IP cumple con las direcciones necesarias para *host* en cada VLANs y se tiene una capacidad de crecimiento.

²⁷ La VLAN para el *stack* de *switches* tiene 30 direcciones IP asignadas no porque las necesite sino porque no se requiere seguir segmentando la red si no hacen falta más direcciones, tomando en cuenta que se han reservando direcciones para crecimiento futuro.

3.3.1.3 Sucursal CST

La Sucursal CST de Quito tiene asignada la dirección de red 192.168.3.0. Para la segmentación en VLANs se realizará el diseño con Subredes y VLSM, y se escogerá la opción que sea viable según la cantidad de direcciones IP necesarias en cada subred.

3.3.1.3.1 Diseño por Subredes

Dirección de Red: 192.168.3.0

Se necesitan 5 subredes:

- Administración
- Stack
- Empleados
- Telefonía IP
- Clientes (Inalámbrico)

192.168.3.00000000

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.3.00000000



Red
Host

$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

En la Sucursal CST se podría aplicar este esquema, con el limitante si crece el número de empleados se podría tener hasta 30 extensiones IP en VLAN de Telefonía.

3.3.1.3.2 Diseño por VLSM

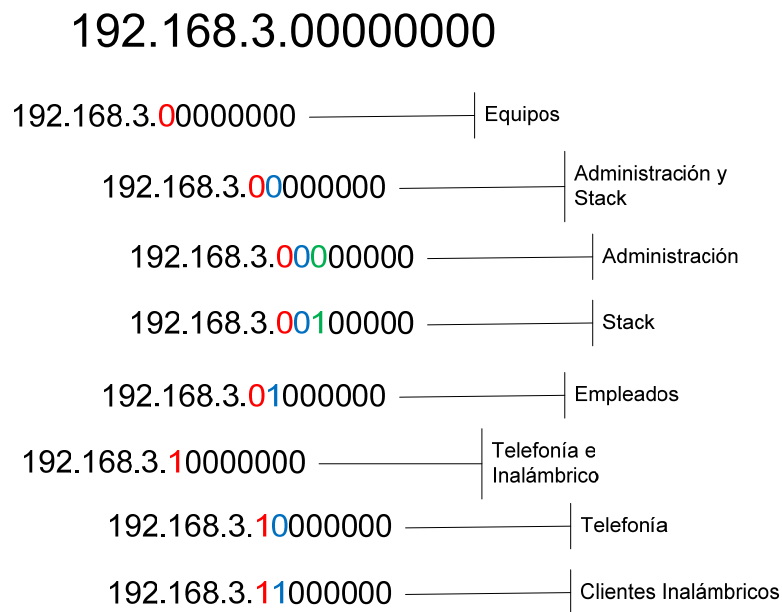


Figura 3-22: Direccionamiento IP Sucursal CST

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.3.0	255.255.255.224	30
Stack	192.168.3.32	255.255.255.224	30
Empleados	192.168.3.64	255.255.255.192	62
Telefonía	192.168.3.128	255.255.255.192	62
Inalámbrico	192.168.3.192	255.255.255.192	62

Tabla 3-31: VLANs Sucursal CST

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	30	7	23
Stack	30	1	29
Empleados	62	27	35
Telefonía	62	23	39
Inalámbrico	62	10	52

Tabla 3-32: Host por VLAN Sucursal CST

Este esquema de direccionamiento cumple con el número de direcciones necesarias para los *host* en cada una de las VLANs y se tiene una capacidad suficiente de crecimiento.

3.3.1.4 Sucursal Sur

La Sucursal Sur de Quito tiene asignada la dirección de red 192.168.4.0. Para la segmentación en VLANs se realizará el diseño con Subredes y VLSM, y se escogerá la opción que sea viable según la cantidad de direcciones IP necesarias en cada subred.

3.3.1.4.1 Diseño por Subredes

Dirección de Red: 192.168.4.0

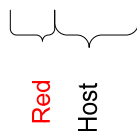
Se necesitan 4 subredes:

- Administración
- Empleados
- Telefonía IP
- Clientes (Inalámbrico)

192.168.4.00000000

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.4.00000000



$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

La Sucursal Sur no tiene tantos empleados como la Sucursal Principal por lo que si se podría aplicar este esquema sin problema.

3.3.1.4.2 Diseño por VLSM

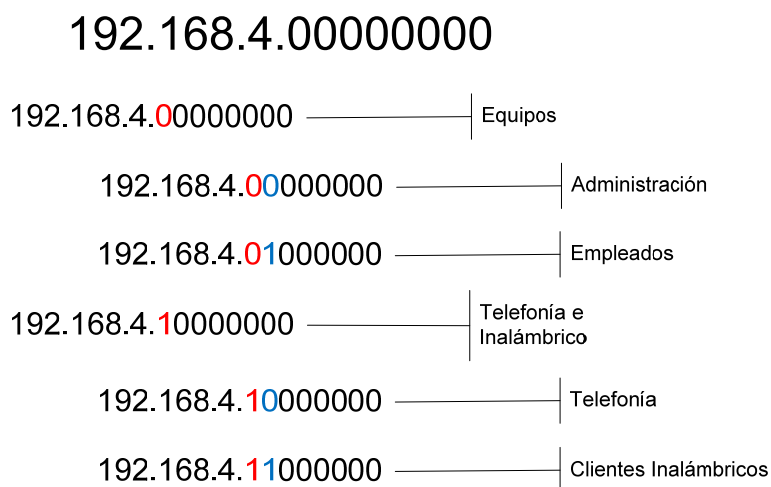


Figura 3-23: Direccionamiento IP Sucursal Sur de Quito

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.4.0	255.255.255.192	62
Empleados	192.168.4.64	255.255.255.192	62
Telefonía	192.168.4.128	255.255.255.192	62
Inalámbrico	192.168.4.192	255.255.255.192	62

Tabla 3-33: VLANs Sucursal Sur de Quito

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	62	2	60
Empleados	62	12	50
Telefonía	62	10	52
Inalámbrico	62	10	52

Tabla 3-34: Host por VLAN Sucursal Sur de Quito

Este esquema de direccionamiento cumple con el número de direcciones necesarias para los *host* en cada una de las VLANs y se tiene una sobrada capacidad de crecimiento.

3.3.2 SUCURSALES DE GUAYAQUIL

A continuación se describen las alternativas de direccionamiento IP, según: Subredes y VLSM, para las sucursales de Guayaquil.

3.3.2.1 Sucursal Mayor

La Sucursal Mayor de Guayaquil tiene asignada la dirección de red 192.168.5.0. Para la segmentación en *VLANs* se realizará el diseño con Subredes y *VLSM*, y se escogerá la opción que sea viable según la cantidad de direcciones *IP* necesarias en cada subred.

3.3.2.1.1 Diseño por Subredes

Dirección de Red: 192.168.5.0

Se necesitan 5 subredes:

- Administración
- *Stack*
- Empleados
- Telefonía *IP*
- Clientes (Inalámbrico)

192.168.5.00000000

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.5.00000000



Red
Host

$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

Se podría aplicar este esquema, con el limitante que si crece el número de extensiones *IP* se podrían tener hasta 30 en la *VLAN* de Telefonía.

3.3.2.1.2 Diseño por VLSM

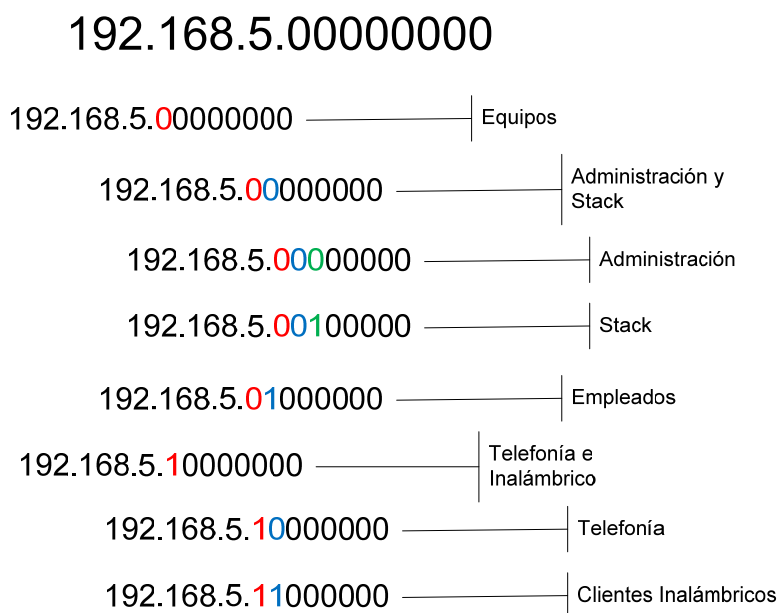


Figura 3-24: Direccionamiento IP Sucursal Mayor

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.5.0	255.255.255.224	30
Stack	192.168.5.32	255.255.255.224	30
Empleados	192.168.5.64	255.255.255.192	62
Telefonía	192.168.5.128	255.255.255.192	62
Inalámbrico	192.168.5.192	255.255.255.192	62

Tabla 3-35: VLANs Sucursal Mayor

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	30	3	27
Stack	30	1	29
Empleados	62	28	34
Telefonía	62	23	39
Inalámbrico	62	10	52

Tabla 3-36: Host por VLAN Sucursal Mayor

Este esquema de direccionamiento cumple con el número de direcciones necesarias para los *host* en cada una de las VLANs y se tiene una capacidad adecuada de crecimiento.

3.3.2.2 Sucursal Sur

La Sucursal Sur de Guayaquil tiene asignada la dirección de red 192.168.6.0. Para la segmentación en VLANs se realizará el diseño con Subredes y VLSM, y se escogerá la opción que sea viable según la cantidad de direcciones IP necesarias en cada subred.

3.3.2.2.1 Diseño por Subredes

Dirección de Red: 192.168.6.0

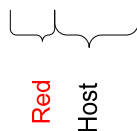
Se necesitan 4 subredes:

- Administración
- Empleados
- Telefonía IP
- Clientes (Inalámbrico)

192.168.6.00000000

$$\text{Subredes} = 2^n - 2 = 2^3 - 2 = 6$$

192.168.6.00000000



$$\text{Host} = 2^n - 2 = 2^5 - 2 = 30 \text{ host/subred}$$

Se podría aplicar este esquema sin problema, con el limitante de que si crece el número de empleados se podrían tener hasta 30 extensiones IP en la VLAN de Telefonía.

3.3.2.2.2 Diseño por VLSM

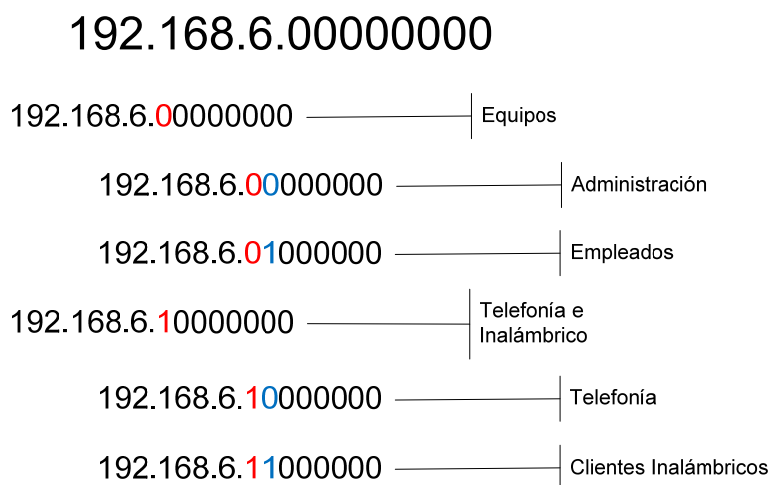


Figura 3-25: Direccionamiento IP Sucursal Sur de Guayaquil

VLAN	Dirección de Subred	Máscara de Subred	# Host / Subred
Administración	192.168.6.0	255.255.255.192	62
Empleados	192.168.6.64	255.255.255.192	62
Telefonía	192.168.6.128	255.255.255.192	62
Inalámbrico	192.168.6.192	255.255.255.192	62

Tabla 3-37: VLANs Sucursal Sur Guayaquil

VLAN	# Host / Subred	# Equipos / VLAN	Capacidad de Crecimiento
Administración	62	3	59
Empleados	62	12	50
Telefonía	62	9	53
Inalámbrico	62	10	52

Tabla 3-38: Host por VLAN Sucursal Sur Guayaquil

El esquema de direccionamiento IP cumple con las direcciones necesarias para *host* en cada VLANs y se tiene una sobrada capacidad de crecimiento.

Como se puede notar VLSM es la única opción viable para la Sucursal Principal por su alto número de empleados; en las demás sucursales se puede utilizar cualquiera de los dos esquemas de direccionamiento. Para manejar un solo esquema de direccionamiento se utilizará VLSM, con esto se gana mayor versatilidad para futuros cambios.

3.4 TELEFONÍA IP INTEGRADA ENTRE SUCURSALES

Las ventajas de las centrales telefónicas IP son:

- Conectar la central a una red IP.
- Tener extensiones IP y adicionalmente que coexistan extensiones analógicas, para fax o Datafast.

Las Centrales Telefónicas deberán manejar estándares de Telefonía IP, como: H.323 y SIP. H.323 es el protocolo que manejan casi todas las centrales telefónicas IP por defecto; éste varía su implementación entre marcas por lo que no garantiza una compatibilidad total. SIP se puede manejar en algunas centrales telefónicas IP comprando licencias adicionales para teléfonos SIP y también existen centrales telefónicas IP SIP, en las cuales todas las extensiones son SIP.

El estándar SIP independiza la marca de la central y de los teléfonos; también permite establecer llamadas entre centrales telefónicas IP compatibles con este protocolo. La ventaja de SIP para este tipo de llamadas es que no se necesita comprar una tarjeta o restringir el número de canales, sino que se pueden realizar llamadas hasta utilizar toda la capacidad del canal.

Los números de extensiones telefónicas tienen tres dígitos, el primero de ellos será utilizado para distinguir las centrales telefónicas de cada sucursal, y los dos restantes servirán para determinar el número de extensión.

Sucursal	Ciudad	Primer número extensión	Números restantes extensión
Principal	Quito	1	00 ... 99
Colón	Quito	2	00 ... 99
CST	Quito	3	00 ... 99
Sur	Quito	4	00 ... 99
Mayor	Guayaquil	5	00 ... 99
Sur	Guayaquil	6	00 ... 99

Tabla 3-39: Asignación de Números de Extensión para llamadas entre Sucursales

La mayoría de Centrales *IP* pueden manejar los siguientes *Codecs*:

- G.711
- G.729
- G.723.1 a 5,3 y 6,3 Kbps

<i>Codec</i>	Velocidad de Bits de Voz	Período de Muestreo	Puntaje Medio de Opinión (MOS)	Payload de Voz	Paquetes por Segundo
G.711	64 Kbps	20 ms	4,3	160 Bytes	50 pps
G.729	8 Kbps	20 ms	3,92	20 Bytes	50 pps
G.723.1	6,3 Kbps	30 ms	3,9	24 Bytes	33,3 pps
G.723.1	5,3 Kbps	30 ms	3,65	20 Bytes	33,3 pps

Tabla 3-40: *Codecs para Telefonía IP*²⁸

Ejemplo de cálculo de capacidad necesaria para redes *LAN* del *Codec G.711* a 20 ms de período de muestreo.

<i>Overhead Ethernet</i>	18 Bytes
Cabecera <i>IP</i>	20 Bytes
Cabecera <i>UDP</i>	8 Bytes
Cabecera <i>RTP</i>	12 Bytes
Payload (Voz)	160 Bytes
Tamaño total por paquete	218 Bytes
Capacidad Esperada	87,2 Kbps

Tabla 3-41: Cálculo de la capacidad G.711 para enlaces *LAN*

$$\text{Capacidad} = \frac{\text{Paquetes}}{\text{segundo}} * \frac{\text{Bytes}}{\text{Paquete}} * \frac{8 \text{ bits}}{1 \text{ byte}}$$

$$\text{Capacidad} = 50 \frac{\text{paquetes}}{\text{s}} * 218 \frac{\text{Bytes}}{\text{paquete}} * 8 \frac{\text{bits}}{\text{Byte}}$$

$$\text{Capacidad} = 87,2 \text{ Kbps}$$

Ejemplo de cálculo de capacidad necesaria para redes *WAN* del *Codec G.711* a 20 ms de período de muestreo y sin compresión:

Cabecera y <i>Trailer</i> Capa 2 (<i>Frame Relay</i>)	6 Bytes
Cabecera <i>IP</i>	20 Bytes
Cabecera <i>UDP</i>	8 Bytes
Cabecera <i>RTP</i>	12 Bytes
Payload (Voz)	160 Bytes
Tamaño total por paquete	206 Bytes
Capacidad Esperada	82,4 Kbps

Tabla 3-42: Cálculo de la capacidad G.711 para enlaces *WAN*

²⁸ Manual de Configuración Central Telefónica *Panasonic TDA-100*

$$Capacidad = \frac{Paquetes}{segundo} * \frac{Bytes}{Paquete} * \frac{8 bits}{1 byte}$$

$$Capacidad = 50 \frac{paquetes}{s} * 206 \frac{Bytes}{paquete} * 8 \frac{bits}{Byte}$$

$$Capacidad = 82,4 Kbps$$

Ejemplo de cálculo de capacidad necesaria para redes WAN del Codec G.711 a 20 ms de Período de Muestreo y con compresión de cabecera (se asume 4 Bytes para la cabecera IP/UDP/RTP):

Cabecera y Trailer Capa 2 (Frame Relay)	6 Bytes
Cabecera IP/UDP/RTP	4 Bytes
Payload (Voz)	160 Bytes
Tamaño total por paquete	170 Bytes
Capacidad Esperada	68 Kbps

Tabla 3-43: Capacidad de Transmisión G.711 para enlaces WAN con compresión

$$Capacidad = \frac{Paquetes}{segundo} * \frac{Bytes}{Paquete} * \frac{8 bits}{1 byte}$$

$$Capacidad = 50 \frac{paquetes}{s} * 170 \frac{Bytes}{paquete} * 8 \frac{bits}{Byte}$$

$$Capacidad = 68 Kbps$$

En la Tabla 3 - 44 se puede observar las capacidades requeridas por los diferentes Codecs para telefonía IP en redes LAN:

Códec	Velocidad de Bits de Voz	Período de Muestreo	Payload de Voz	Paquetes por Segundo	LAN (Ethernet)
G.711	64 Kbps	20 ms	160 Bytes	50 pps	87,2 Kbps
G.711	64 Kbps	30 ms	240 Bytes	33,3 pps	79,5 Kbps
G.711	64 Kbps	40 ms	320 Bytes	25 pps	75,6 Kbps
G.729	8 Kbps	20 ms	20 Bytes	50 pps	31,2 Kbps
G.729	8 Kbps	30 ms	30 Bytes	33,3 pps	23,5 Kbps
G.729	8 Kbps	40 ms	40 Bytes	25 pps	19,6 Kbps
G.723.1	6,3 Kbps	30 ms	24 Bytes	33,3 pps	21,8 Kbps
G.723.1	6,3 Kbps	60 ms	47 Bytes	16,7 pps	14,0 Kbps
G.723.1	6,3 Kbps	90 ms	71 Bytes	11,1 pps	11,5 Kbps
G.723.1	5,3 Kbps	30 ms	20 Bytes	33,3 pps	20,8 Kbps
G.723.1	5,3 Kbps	60 ms	40 Bytes	16,7 pps	13,0 Kbps
G.723.1	5,3 Kbps	90 ms	60 Bytes	11,1 pps	10,5 Kbps

Tabla 3-44: Valores de Capacidad LAN Codecs Telefonía IP

En la Tabla 3 - 45 se puede observar las capacidades requeridas por los diferentes *Codecs* para telefonía *IP* en redes *WAN*:

Código	Velocidad de Bits de Voz	Período de Muestreo	Payload de Voz	Paquetes por Segundo	WAN (FRAME RELAY)	
					RTP	cRTP
G.711	64 Kbps	20 ms	160 Bytes	50 pps	82,4 Kbps	68,0 Kbps
G.711	64 Kbps	30 ms	240 Bytes	33,3 pps	76,3 Kbps	66,7 Kbps
G.711	64 Kbps	40 ms	320 Bytes	25 pps	73,2 Kbps	66,0 Kbps
G.729	8 Kbps	20 ms	20 Bytes	50 pps	26,4 Kbps	12 Kbps
G.729	8 Kbps	30 ms	30 Bytes	33,3 pps	20,3 Kbps	10,7 Kbps
G.729	8 Kbps	40 ms	40 Bytes	25 pps	17,2 Kbps	10,0 Kbps
G.723.1	6,3 Kbps	30 ms	24 Bytes	33,3 pps	18,6 Kbps	9,0 Kbps
G.723.1	6,3 Kbps	60 ms	47 Bytes	16,7 pps	12,4 Kbps	7,6 Kbps
G.723.1	6,3 Kbps	90 ms	71 Bytes	11,1 pps	10,5 Kbps	7,2 Kbps
G.723.1	5,3 Kbps	30 ms	20 Bytes	33,3 pps	17,6 Kbps	8 Kbps
G.723.1	5,3 Kbps	60 ms	40 Bytes	16,7 pps	11,4 Kbps	6,6 Kbps
G.723.1	5,3 Kbps	90 ms	60 Bytes	11,1 pps	9,4 Kbps	6,2 Kbps

Tabla 3-45: Valores de capacidad WAN Codecs Telefonía IP

Las centrales telefónicas generalmente soportan los cuatro estándares (G.711, G.723.1 a 6,3 o 5,3 Kbps y G.729), el fabricante recomienda que se utilice cualquiera de ellos pero con el menor período de muestreo, para que las conversaciones telefónicas no sean entrecortadas o con voz robotizada. Adicionalmente, se recomienda el correcto dimensionamiento de los canales para que se garantice la capacidad requerida por el estándar escogido.

El estándar escogido según su calidad y nitidez en relación a la capacidad necesaria es G.729 a 8 Kbps, tiene un MOS de 3.92. La telefonía *IP* que se realice fuera de una sucursal o de la empresa, utilizando los enlaces entre sucursales e *Internet* se calcularán con este estándar.

Para telefonía dentro una misma sucursal se utilizará el Código G.711, el cual tiene el MOS 4.3 que es el más alto entre todos los *Codecs*. Dentro de la red *LAN* se busca más la calidad de la comunicación antes que una baja capacidad requerida.

Se va a tomar en cuenta estas recomendaciones y se utilizará para el diseño:

Código	Velocidad de Bits de Voz	Período de Muestreo	Puntaje Medio de Opinión (MOS)	LAN (Ethernet)	WAN (FRAME RELAY)	
					RTP	cRTP
G.711	64 Kbps	20 ms	4.3	87,2 Kbps	82,4 Kbps	68 Kbps
G.729	8 Kbps	20 ms	3,92	31,2 Kbps	26,4 Kbps	12 Kbps

Tabla 3-46: Codecs Recomendados para el Diseño del Sistema de Telefonía IP

3.4.1 EQUIPOS NECESARIOS PARA TELEFONÍA IP

Para manejar Telefonía IP en una empresa es necesario tener: Centrales Telefónicas IP y teléfonos IP compatibles con las centrales. En estas centrales se pueden instalar tarjetas FXO, para conectar líneas analógicas y FXS, para conectar teléfonos analógicos o máquinas de fax o Datafast.

3.4.1.1 Centrales Telefónicas

Las Centrales Telefónicas IP deben cumplir con estas especificaciones:

- Compatibilidad con SIP y H.323
- Compatibilidad con SNMP
- Puertos FXO y FXS: 4 o más.
- Compatibilidad con Codecs: G.711, G.729

Las centrales telefónicas deben cumplir con todas las especificaciones requeridas para tener un sistema de Telefonía IP de punta y administrable con el Sistema de Administración de Red que se va a utilizar.

Sucursal	Ciudad	Cantidad	Central Telefónica	Usuarios	COs
Principal	Quito	1	Central Telefónica IP	39	21
Colón	Quito	1	Central Telefónica IP	17	15
CST	Quito	1	Central Telefónica IP	23	14
Sur	Quito	1	Central Telefónica IP	11	8
Mayor	Guayaquil	1	Central Telefónica IP	23	9
Sur	Guayaquil	1	Central Telefónica IP	9	6
TOTAL		6			

Tabla 3-47: Usuarios y COs de las Centrales Telefónicas

Todas las sucursales por más pequeñas que sean deben tener una central telefónica; no se pueden utilizar extensiones de otra sucursal para una sucursal pequeña porque al no poder recibir llamadas de sus clientes, la empresa pierde mucho más que el precio de las mismas centrales telefónicas.

3.4.1.2 Teléfonos *IP*

Los teléfonos *IP* deben cumplir con las siguientes especificaciones:

- Compatibilidad con el estándar *SIP* y *H.323*
- 2 puertos 10/100 *Base T*
- Compatibilidad con *PoE* (802.3af)
- Compatibilidad con *Códecs*: *G.711*, *G.729*

Sucursal	Ciudad	Cantidad	Teléfono
Principal	Quito	39	Teléfono <i>IP</i>
Colón	Quito	17	Teléfono <i>IP</i>
CST	Quito	23	Teléfono <i>IP</i>
Sur	Quito	11	Teléfono <i>IP</i>
Mayor	Guayaquil	23	Teléfono <i>IP</i>
Sur	Guayaquil	9	Teléfono <i>IP</i>
	TOTAL	122	

Tabla 3-48: Número de Teléfonos por Sucursal

Es necesario que los teléfonos cumplan las especificaciones antes descritas, para integrarlos a la infraestructura existente sin tener que incrementar puntos de red para voz y cableado eléctrico.

Adicionalmente, los teléfonos deben ser compatibles con los *codecs* de voz establecidos, para cumplir con los cálculos de capacidad de los enlaces entre sucursales realizados en base a estos *codecs*.

3.4.2 ENLACES PARA TELEFONÍA IP

3.4.2.1 Enlace Sucursal Principal – CST

Este enlace es de fibra óptica y propio de la empresa; los equipos utilizados para el enlace son los que se muestran en la Figura 3-26:

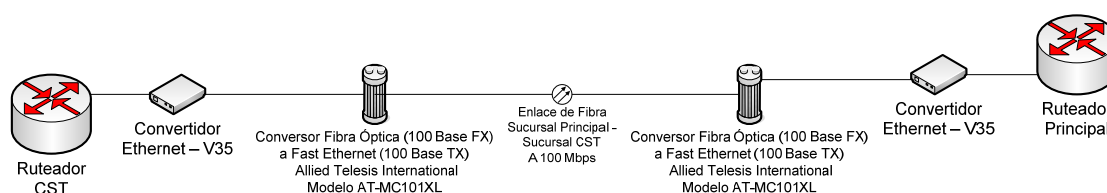


Figura 3-26: Enlace Sucursal Principal - CST

Los cálculos para el dimensionamiento de este enlace se realizarán con los datos de redes LAN porque la tecnología del enlace no es WAN.

Los canales para VoIP que se van a utilizar para llamadas fuera de la Sucursal Principal son 12. Para la Sucursal CST se van a habilitar 8 canales que son menores a los 12 canales de la Sucursal Principal.

Sucursal Principal (Quito)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	8	8	4
Ventas	9	9	2
Bodega	5	2	0
Crédito	5	5	2
Auditoría Externa	2	1	1
Caja	3	1	0
Contabilidad	3	2	1
Técnico	2	1	1
Sistemas	2	1	1
Datafast	0	3	0
TOTAL	39	33	12

Tabla 3-49: Dimensionamiento de Canales Telefonía IP Sucursal Principal

En la Sucursal Principal trabajan 39 personas que necesitan comunicarse con personas de otras sucursales, llamar a otras ciudades o países. Por lo cual, la *VoIP* reduciría los costos de llamadas nacionales e internacionales.

El dimensionamiento se lo realizó por el número de empleados de los departamentos que podrían necesitar comunicarse con otras sucursales, ciudades u otros países. Queda claro que éste no es un impedimento para utilizar estos servicios las personas que no estén en los departamentos y no tengan asignados canales para *VoIP*, sino que solo se utilizó esta política para el dimensionamiento de los canales de *VoIP*.

Cada empleado tendrá un perfil de usuario en la central telefónica donde se le permitirá o se le restringirá las llamadas nacionales, regionales o internacionales. Adicionalmente cada empleado tendrá una clave para acceder a una línea externa, con lo cual se llevará un registro de llamadas, duración de llamadas, etc.

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ LAN} * n_{canales\ LAN}$$

$$Capacidad_T = 31,2\ kbps * 12 = 374,40\ Kbps$$

3.4.2.2 Enlace Sucursal CST – Colón

Este enlace inalámbrico usa *access points* 802.11g, el mismo que por su distancia y características alcanza una velocidad de 5,5 *Mbps*²⁹, mediante antenas parabólicas de 24 *dBi* instaladas en las sucursales. Este enlace se logra por medio de *access points* repetidores en el Volcán Pichincha y *access points* que están en cada sucursal que conforman este enlace.

²⁹ Utilizando el programa de administración de capacidad de transmisión *MRTG* se conoció la capacidad de transmisión máxima del enlace y se supone que ésta es su capacidad.

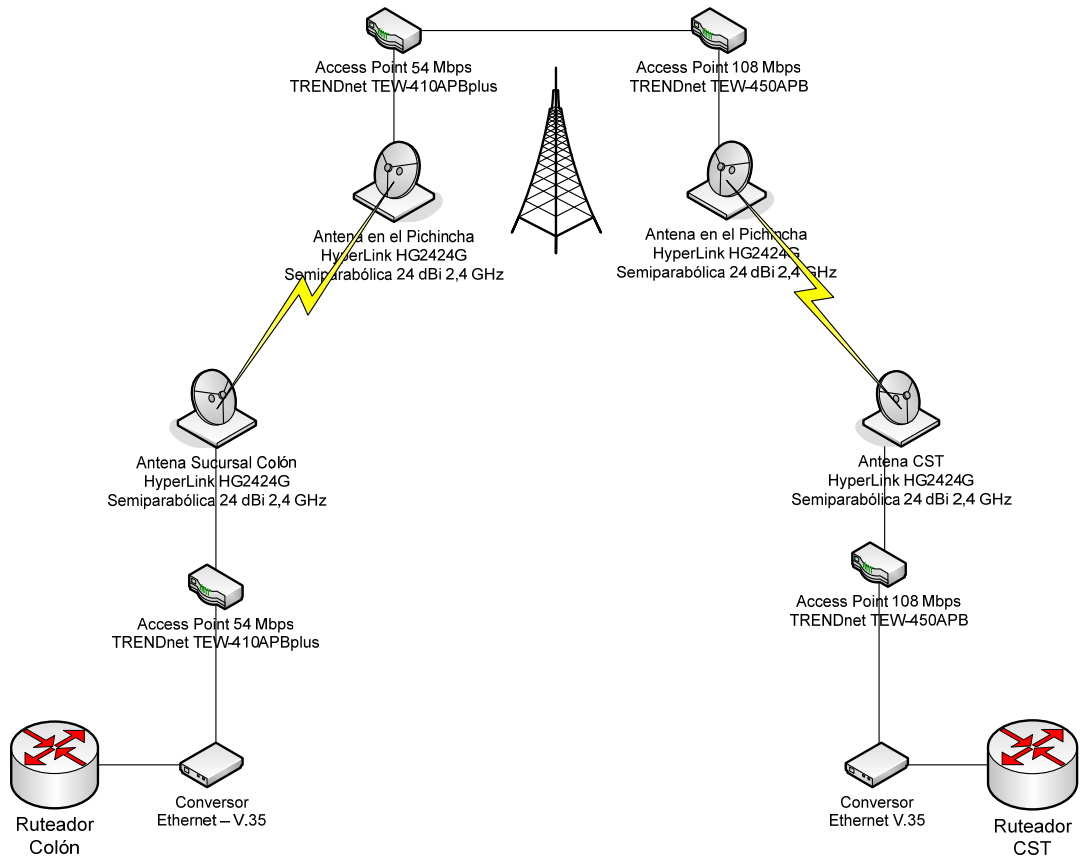


Figura 3-27: Enlace Sucursal CST- Colón

Los cálculos para el dimensionamiento de este enlace se realizarán con los datos de redes LAN porque no se utilizó una tecnología WAN para su implementación. El dimensionamiento de los canales para VoIP se realizó tomando en cuenta los departamentos que pueden necesitar este servicio, tal como se muestra en la Tabla 3 - 50.

Sucursal Colón (Quito)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	2	2	2
Bodega	3	2	0
Caja	2	1	0
Crédito	2	2	1
Ventas	7	7	4
Técnico	1	1	1
Datafast	0	1	0
TOTAL	17	16	8

Tabla 3-50: Dimensionamiento Canales Telefonía IP Sucursal Colón

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ LAN} * n_{canales\ LAN}$$

$$Capacidad_T = 31,2\ kbps * 8 = 249,60\ Kbps$$

Este enlace va a ser utilizado para llamadas salientes de la Sucursal Colón y para recibir llamadas de otras sucursales de la empresa o fuera de ella. No se puede dar el caso de que todas las líneas de salida de la Sucursal Principal (12 canales *VoIP*) necesiten llamar a la Sucursal Colón, por lo que no se necesita un cálculo de canales extra.

3.4.2.3 Enlace Sucursal CST – Sur (Quito)

Este enlace inalámbrico usa *access points* 802.11g, que por la distancia y las características del mismo alcanzan una velocidad de 1 *Mbps*³⁰, gracias a las antenas parabólicas de 24 *dBi* instaladas en las sucursales de la empresa.

Sucursal Sur (Quito)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	2	2	1
Bodega	2	1	0
Caja	2	1	0
Ventas	4	4	2
Técnico	1	1	1
Datafast	0	1	0
TOTAL	11	10	4

Tabla 3-51: Dimensionamiento Canales Telefonía IP Sucursal Sur de Quito

En la Figura 3-28 se muestra el esquema de los equipos del enlace entre las sucursales Sur – CST, que también será utilizados para implementar telefonía *IP*.

³⁰ Utilizando el programa de administración de la capacidad de transmisión *MRTG* se conoció la capacidad de transmisión máxima del enlace y se supone que ésta es su capacidad.

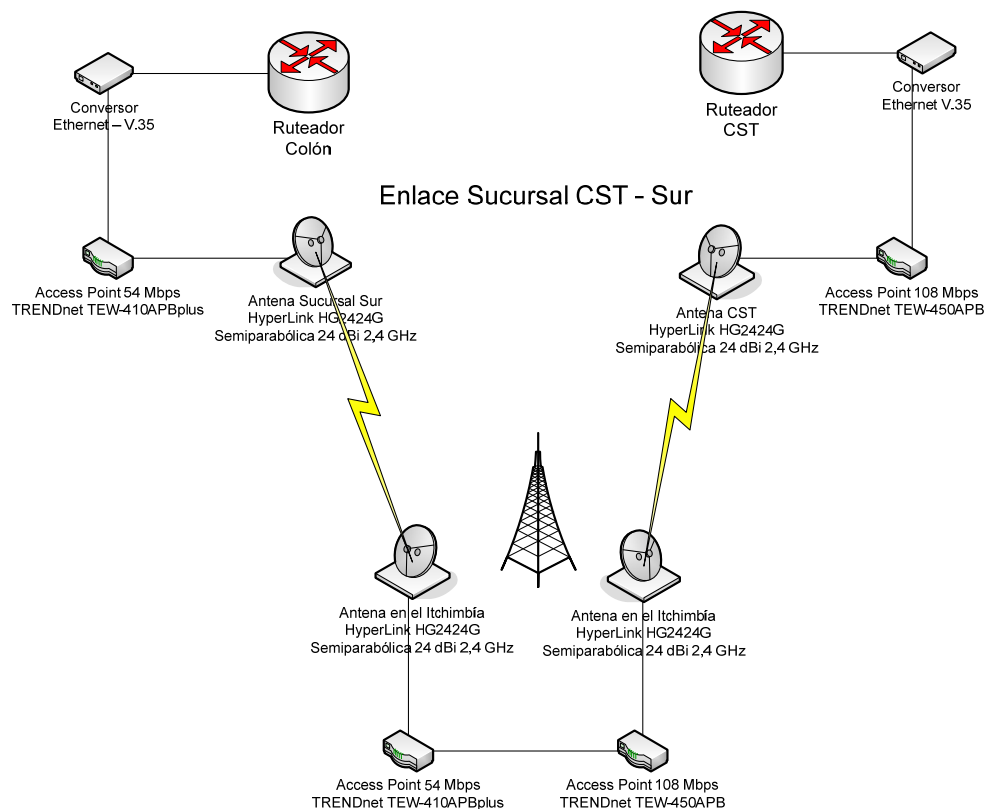


Figura 3-28: Enlace Sucursal CST - Sur

Los cálculos para el dimensionamiento de este enlace se realizarán con los datos de redes LAN, porque no se tiene una tecnología WAN en los enlaces privados. Los canales para VoIP que se van a utilizar para llamadas fuera de la Sucursal Sur de Quito son 4.

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ LAN} * n_{canales\ LAN}$$

$$Capacidad_T = 31,2\ kbps * 4 = 124,80\ Kbps$$

Este enlace va a ser utilizado para llamadas salientes de la Sucursal Sur y para recibir llamadas de otras sucursales de la empresa o de fuera de ella. No se puede dar el caso de que todas las líneas de salida de la Sucursal CST (8 canales VoIP) necesiten llamar a la Sucursal Sur, por lo que no se ha tomando en cuenta este caso para el dimensionamiento del enlace.

3.4.2.4 Enlace Sucursal Mayor (Guayaquil) – CST (Quito)

Los cálculos para el dimensionamiento de este enlace se realizarán con los datos de redes *WAN*, porque este enlace será contratado a un proveedor de servicios, ya que implementar un enlace privado de tal distancia implica costos muy altos.

Los canales para *VoIP* que se van a utilizar para llamadas fuera de la Sucursal Mayor de Guayaquil son 8, según la Tabla 3-52 utilizada para el dimensionamiento del número de canales de salida de esta sucursal.

Sucursal Mayor (Guayaquil)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	3	3	2
Bodega	4	1	0
Caja	2	1	0
Contabilidad	1	1	0
Crédito	1	1	1
Mercadeo	2	1	1
Técnico	3	2	1
Ventas	7	7	3
Datafast	0	1	0
TOTAL	23	18	8

Tabla 3-52: Dimensionamiento Canales Telefonía IP Sucursal Mayor de Guayaquil

Los canales para *VoIP* que se van a utilizar para llamadas fuera de la Sucursal CST de Quito son 8, según la Tabla 3 - 53 utilizada para el dimensionamiento del número de canales de salida de esta sucursal.

Sucursal CST (Quito)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	2	2	1
Caja	1	1	0
Garantías	2	2	1
Mercadeo	7	5	3
Sistemas	1	1	1
Técnico	10	6	2
TOTAL	23	18	8

Tabla 3-53: Dimensionamiento Canales Telefonía IP Sucursal CST Quito

Para el enlace entre Quito y Guayaquil se tendrán 8 canales *IP* para las llamadas entre las sucursales; las llamadas que no sean entre Quito y Guayaquil serán enrutadas por la ciudad donde se tenga menor costo de llamada, para que sea una llamada regional y no una nacional. Las llamadas nacionales deben salir por la ciudad de origen y las llamadas a otros países se las enrutará por *Internet*.

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ WAN} * n_{canales\ WAN}$$

$$Capacidad_T = 26,4\ kbps * 8 = 211,20\ Kbps$$

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ LAN} * n_{canales\ LAN}$$

$$Capacidad_T = 31,2\ kbps * 8 = 249,60\ Kbps$$

3.4.2.5 Enlace Sucursal Mayor – Sur (Guayaquil)

Este enlace hasta el momento no existe, por lo que en el Capítulo 4 se decidirá la tecnología para el enlace de las alternativas para contratarlo. Los cálculos para el dimensionamiento se realizarán con los datos de redes *WAN*.

Los canales para *VoIP* que se van a utilizar para llamadas fuera de la Sucursal Sur de Guayaquil son 4, según la Tabla 3-54 utilizada para el dimensionamiento del número de canales de salida de esta sucursal.

Sucursal Sur (Guayaquil)			
Departamento	# Personas	# Extensiones	# Canales VoIP
Administrativo	2	2	1
Bodega	2	2	0
Caja	1	1	0
Ventas	3	3	2
Técnico	1	1	1
Datafast	0	1	0
TOTAL	9	10	4

Tabla 3-54: Dimensionamiento Canales VoIP Sucursal Sur de Guayaquil

$$Capacidad_T = Capacidad_{1\ canal\ G.729\ WAN} * n_{canales\ WAN}$$

$$Capacidad_T = 26,4\ kbps * 4 = 105,60\ Kbps$$

Este enlace va a ser utilizado para salida de las llamadas de la Sucursal Sur de Guayaquil y para recibir llamadas de otras sucursales o de fuera de ella.

No se puede dar el caso de que todas las líneas de salida de la Sucursal Mayor de Guayaquil (8 canales *VoIP*) necesiten llamar a la Sucursal Sur de Guayaquil, por lo que no se ha tomando en cuenta este caso para el dimensionamiento del enlace.

En la Tabla 3- 55 se presenta un resumen de la capacidad de transmisión necesaria para cada enlace según el códec G.729 y el número de canales determinados por el diseño según las necesidades de cada sucursal.

Sucursal	Ciudad	# Canales VoIP	Tipo de Enlace	Capacidad G.729 a 8 Kbps
Principal	Quito	12	LAN	374,40 Kbps
Colón	Quito	8	LAN	249,60 Kbps
CST	Quito	8	LAN	249,60 Kbps
Sur	Quito	4	LAN	124,80 Kbps
Mayor	Guayaquil	8	WAN	211,20 Kbps
Sur	Guayaquil	4	WAN	105,60 Kbps

Tabla 3-55: Resumen Canales Telefonía IP Sucursales

3.4.3 VIDEOCONFERENCIA IP

La videoconferencia *IP* entre las sucursales de la empresa, la utilizarán los gerentes o ejecutivos para comunicarse dentro de la empresa y fuera de ella. Cada sucursal tiene número limitado de canales para videoconferencias, dado que este servicio es costoso por los enlaces entre las sucursales y la salida a *Internet* que se necesitan.

Al ser la videoconferencia *IP* una aplicación de tiempo real se debe reservar la capacidad para su correcta ejecución; se tienen algunas resoluciones y tasas de cuadros por segundo, que varía la capacidad necesaria para la videoconferencia.

Los videoteléfonos se instalarán en cada una de las Gerencias de las Sucursales, en caso de necesitarse para una videoconferencia se instalará el videoteléfono en el auditorio o sala de reuniones de la sucursal. Una vez instalado no se necesita cambiar la configuración del videoteléfono y como se tiene puntos de red en cada auditorio o sala de reuniones solamente se conecta y se establece la videoconferencia.

Cada sucursal tendrá un solo canal para videoconferencia; entre Quito y Guayaquil se ha previsto una sola videoconferencia sobre *Internet*, es decir se pueden realizar video llamadas entre las sucursales (una por sucursal), y solo una por el enlace entre Quito y Guayaquil.

Los equipos para videoconferencia deben cumplir con los estándares:

- *H.323 o SIP*
- *H.263 o H.264*
- *G.711, G.729*
- *CIF o QCIF*

En la Tabla 3 - 56 se detalla la capacidad de transmisión de videoconferencia con el códec *H.264* en relación con la resolución del video y el número de cuadros por segundo.

Capacidad de Transmisión	Resolución y cuadros por segundo
128 <i>Kbps</i>	128 X 96 pixeles y 30,9 cuadros por segundo 176 X 144 pixeles y 15,0 cuadros por segundo
192 <i>Kbps</i>	176 X 144 pixeles y 30,3 cuadros por segundo 320 X 240 pixeles y 10,0 cuadros por segundo
384 <i>Kbps</i>	320 X 240 pixeles y 20,0 cuadros por segundo 352 X 288 pixeles y 15,2 cuadros por segundo

Tabla 3-56: Capacidad de Transmisión Vs. Resolución y Cuadros por segundo³¹

Para el dimensionamiento de los enlaces se tomará 192 *Kbps* como capacidad para videoconferencia *IP*, por no requerir mucha capacidad de transmisión y tener una buena resolución.

³¹ Obtenido de la página web de <http://es.wikipedia.org/wiki/H.264>

3.5 CÁLCULO ENLACE *INTERNET* Y ENLACES ENTRE SUCURSALES

Los enlaces entre las sucursales son utilizados para tráficos de voz, datos y video; más específicamente para transmitir, los siguientes tipos de tráfico:

- Consultas de bases de datos
- Consolidación de datos de la *Intranet*
- Enviar correo interno y externo
- Administración y ejecución del Sistema Antivirus Corporativo
- Administración remota de la red
- Telefonía y Videoconferencia *IP*
- Acceso a *Internet*, para navegación
- Mensajería Instantánea
- Transferencia de archivos

Todos estos tipos de tráfico deben ser tomados en cuenta para el dimensionamiento de los enlaces entre las sucursales y la salida a *Internet* según el tráfico de cada uno de los enlaces.

3.5.1 CÁLCULO CAPACIDAD DE SALIDA A *INTERNET*

Los cálculos para el dimensionamiento de la salida hacia *Internet* en Quito y Guayaquil son referenciales, cuando se implemente este proyecto se deberá probar los enlaces con las especificaciones de este estudio y tomar decisiones para quedarse con las capacidades sugeridas o modificarlas.

El factor de compartición del acceso a *Internet* es un punto muy importante a tomar en cuenta, ya que no es lo mismo un canal con compartición 4:1, 2:1 o 1:1. Para empresas se recomienda este tipo de factores de compartición, mientras más usuarios debe ser menor el factor de compartición y se tiene que incrementar la capacidad del canal, logrando así un mejor servicio.

3.5.1.1 Sucursales de Quito

La salida a *Internet* de las Sucursales de Quito se instalará en la Sucursal CST, donde se encuentra el administrador de la red y los técnicos de la empresa. En caso de fallas, esta sucursal es estratégica para la solución de problemas en el menor tiempo posible; adicionalmente en esta sucursal se tienen instalados equipos de los enlaces de las sucursales.

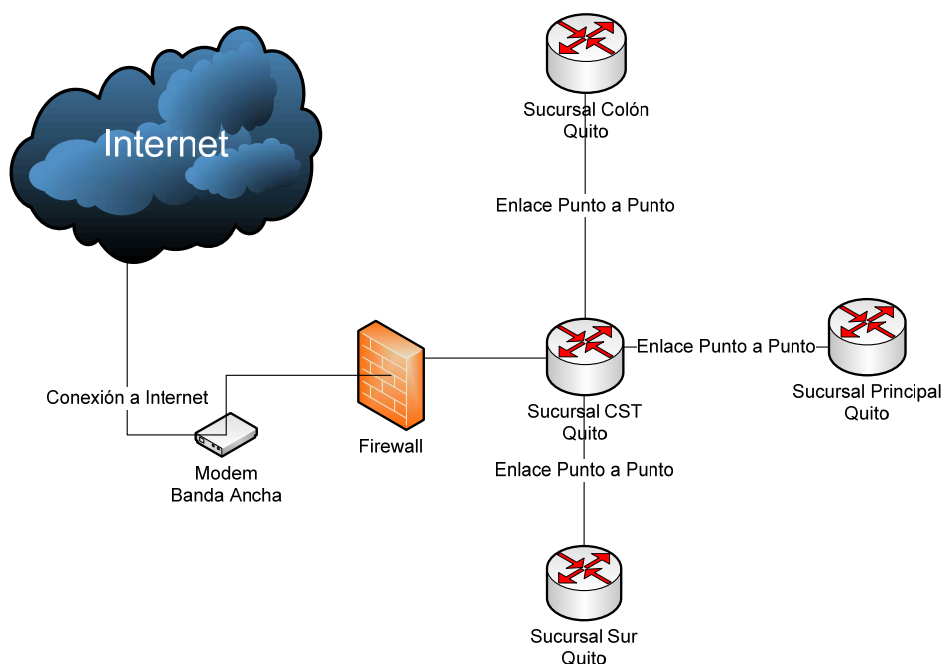


Figura 3-29: Esquema Conexión a *Internet* de Quito

Sucursales de Quito			
Sucursal	# Personas	# Personas con Acceso a <i>Internet</i>	Capacidad Requerida
Principal	39	28	714,00 Kbps
Colón	17	12	306,00 Kbps
CST	23	20	510,00 Kbps
Sur	11	7	178,50 Kbps
TOTAL	90	67	1708,50 Kbps

Tabla 3-57: Cálculo de Capacidad *Internet* Quito

Las capacidades de transmisión mostradas en la Tabla 3 - 57 son los resultados de los cálculos que se realizan posteriormente en este capítulo.

Casi todos los proveedores usan redes *ATM* sobre *SDH* con el enlace de última milla *ADSL* para brindar servicios de *Internet* a sus clientes, entonces se va a calcular el porcentaje de *overhead* en este tipo de redes para el dimensionamiento de la capacidad de *Internet* necesaria.

OC-3c (en Mbps)				
Velocidad de la Línea	155,52			
SONET Payload	149,76			Disponible ATM
ATM Payload	135,63			Disponible AAL
MTU	576 Bytes	9180 Bytes	65527 Bytes	
AAL5 Payload	126,94	135,22	135,56	Disponible LLC/SNAP
LLC/SNAP Payload	125,20	135,10	135,55	Disponible IP
IP Payload	120,85	134,81	135,51	Disponible Transporte
UDP Payload	119,11	134,69	135,49	Disponible Aplicación
TCP Payload	116,50	134,51	135,46	Disponible Aplicación ³²

Tabla 3-58: Capacidad ATM sobre SDH

$$\%Overhead_{TCP} = 100\% - \left(\frac{V_{Línea}}{V_{Capa\ Aplicación\ TCP}} * 100\% \right)$$

$$\%Overhead_{TCP} = 100\% - \left(\frac{116,50\ Mbps}{155,52\ Mbps} * 100\% \right) = 25\%$$

$$\%Overhead_{UDP} = 100\% - \left(\frac{V_{Línea}}{V_{Capa\ Aplicación\ UDP}} * 100\% \right)$$

$$\%Overhead_{UDP} = 100\% - \left(\frac{119,11\ Mbps}{155,52\ Mbps} * 100\% \right) = 23\%$$

Para los cálculos de la capacidad se asume un *overhead* del 25% de los datos útiles, y adicionalmente se incluirá el 10% de tolerancia.

$$Capacidad_{Total} = Capacidad_{Sucursales} + Capacidad_{videoconferencia}$$

$$Capacidad_{Total} = 1708,50\ Kbps + 240\ Kbps = 1948,50\ Kbps$$

$$Capacidad_{Necesario} = Capacidad_{Total} * 1,1$$

$$Capacidad_{Necesario} = 1948,50\ Kbps * 1,1 = 2143,35\ Kbps$$

La capacidad total aproximada es 2,048 Mbps porque es la capacidad estándar que tienen los proveedores de *Internet*, y no varía sustancialmente la capacidad calculada.

³² Tabla obtenida de *Protocol Overhead* en <http://sd.wareonearth.com/~phil/net/overhead/>

3.5.1.1.1 Sucursal Principal

Los usuarios que tienen conexión a *Internet* por departamento, son:

Sucursal Principal (Quito)			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	8	Si	8
Ventas	9	Si	9
Sistemas	2	Si	2
Crédito	5	Si	5
Auditoría Externa	2	Si	2
Caja	3	No	0
Contabilidad	3	No	0
Bodega	5	No	0
Técnico	2	Si	2
TOTAL	39		28

Tabla 3-59: Acceso a *Internet* Sucursal Principal Quito

En esta sucursal existen 28 usuarios conectados a *Internet*, su aplicación es:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{\text{usuario página web}}^{33} = T_{\text{página}} * t_{\text{carga}}$$

$$C_{\text{usuario página web}} = 40 \frac{\text{KB}}{\text{página}} * \frac{1 \text{ página}}{5 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 64 \text{ Kbps}$$

$$C_{\text{Navegar}} = \# \text{usuarios} * I_{\text{simultaneidad}}^{34} * C_{\text{usuario página web}}$$

$$C_{\text{Navegar}} = 28 * 0,15 * 64 \text{ Kbps} = 268,80 \text{ Kbps}$$

Se asume: que una página *web* promedio tiene 40 KB y el tiempo de carga es 5 segundos. El índice de simultaneidad dado el tipo de empresa se asume que el 15% de los usuarios cargan una página *web* simultáneamente.

³³ C= Capacidad

³⁴ *I_{Simultaneidad} = Índice de Simultaneidad

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM\ usuario}^{35}$$

$$C_{IM} = 28 * 2\ Kbps = 56\ Kbps$$

Se asume que todos los usuarios conectados a *Internet* utilizan algún programa de mensajería instantánea para comunicación interna o externa.

Tráfico de Correo electrónico:

$$C_{usuario\ email} = T_{email} * t_{descarga}$$

$$C_{usuario\ email} = 30 \frac{KB}{email} * \frac{1\ email}{5\ segundos} * \frac{8\ bits}{1\ Byte} = 48\ Kbps$$

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ email}$$

$$C_{Email} = 28 * 0,1 * 48\ Kbps = 134,40\ Kbps$$

Se asume que cada correo electrónico promedio tiene 30 KB y un índice de simultaneidad del 10%.

Descarga de Archivos:

$$C_{usuario\ descarga\ archivo} = T_{archivo} * t_{descarga}$$

$$C_{usuario\ descarga\ archivo} = 300 \frac{KB}{archivo} * \frac{1\ archivo}{60\ segundos} * \frac{8\ bits}{1\ Byte} = 40\ Kbps$$

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ descarga\ archivo}$$

$$C_{Descargar} = 28 * 0,1 * 40\ Kbps = 112\ Kbps$$

Un archivo de 300 KB que se descargue en 60 segundos, se asume como un buen tiempo de descarga. Se asume un $I_{simultaneidad}$ del 10%.

³⁵ El $C_{IM\ usuario} = 2\ Kbps$ es el promedio de la capacidad de transmisión para Mensajería Instantánea por usuario que *Microsoft* publicó en www.microsoft.com/technet

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 268,80 \text{ Kbps} + 56 \text{ Kbps} + 134,40 \text{ Kbps} + 112 \text{ Kbps}$$

$$C_T = 571,20 \text{ Kbps} * 1,25^{36} = 714,00 \text{ Kbps}$$

3.5.1.1.2 Sucursal Colón

Los usuarios de la Sucursal Colón que utilizan *Internet* por departamento son:

Sucursal Colón (Quito)			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	2	Si	2
Ventas	7	Si	7
Bodega	3	No	0
Técnico	1	Si	1
Caja	2	No	0
Crédito	2	Si	2
TOTAL	17		12

Tabla 3-60: Acceso a *Internet* Sucursal Colón Quito

En esta sucursal se tiene un total de 12 usuarios que utilizan *Internet*; las principales aplicaciones que le dan a este servicio son:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{Navegar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ página web}}$$

$$C_{Navegar} = 12 * 0,15 * 64 \text{ Kbps} = 115,20 \text{ Kbps}$$

El ancho de banda de 64 Kbps es el resultado de que una página 40 KB se cargue en 5 segundos, lo cual se asume.

³⁶ El 25% de la carga útil se supone un promedio de *overhead* para redes WAN

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM\ usuario}$$

$$C_{IM} = 12 * 2\ Kbps = 24\ Kbps$$

Tráfico de Correo electrónico:

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ email}$$

$$C_{Email} = 12 * 0,1 * 48\ Kbps = 57,60\ Kbps$$

Descarga de Archivos:

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ descarga\ archivo}$$

$$C_{Descargar} = 12 * 0,1 * 40\ Kbps = 48\ Kbps$$

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 115,20\ Kbps + 24\ Kbps + 57,60\ Kbps + 48\ Kbps$$

$$C_T = 244,80\ Kbps * 1,25 = 306,00\ Kbps$$

3.5.1.1.3 Sucursal CST

Los usuarios de la Sucursal CST que utilizan *Internet* por departamento son:

Sucursal CST (Quito)			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	2	Si	2
Mercadeo	7	Si	7
Sistemas	1	Si	1
Caja	1	No	0
Garantías	2	No	0
Técnico	10	Si	10
TOTAL	23		20

Tabla 3-61: Acceso a *Internet* Sucursal CST Quito

En esta sucursal existen 20 usuarios conectados a *Internet*, su aplicación es:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{Navegar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ página web}}$$

$$C_{Navegar} = 20 * 0,15 * 64 \text{ Kbps} = 192 \text{ Kbps}$$

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM \text{ usuario}}$$

$$C_{IM} = 20 * 2 \text{ Kbps} = 40 \text{ Kbps}$$

Tráfico de Correo electrónico:

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ email}}$$

$$C_{Email} = 20 * 0,1 * 48 \text{ Kbps} = 96 \text{ Kbps}$$

Descarga de Archivos:

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ descarga archivo}}$$

$$C_{Descargar} = 20 * 0,1 * 40 \text{ Kbps} = 80 \text{ Kbps}$$

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 192 \text{ Kbps} + 40 \text{ Kbps} + 96 \text{ Kbps} + 80 \text{ Kbps}$$

$$C_T = 408,00 \text{ Kbps} * 1,25 = 510,00 \text{ Kbps}$$

3.5.1.1.4 Sucursal Sur

Los usuarios de la Sucursal Sur que utilizan *Internet* por departamento son:

Sucursal Sur (Quito)			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	2	Si	2
Ventas	4	Si	4
Caja	2	No	0
Bodega	2	No	0
Técnico	1	Si	1
TOTAL	11		7

Tabla 3-62: Acceso a *Internet* Sucursal Sur Quito

En esta sucursal se tiene un total de 7 usuarios que utilizan *Internet*, las principales aplicaciones que le dan a este servicio son:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{Navegar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ página web}}$$

$$C_{Navegar} = 7 * 0,15 * 64 \text{ Kbps} = 67,20 \text{ Kbps}$$

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM \text{ usuario}}$$

$$C_{IM} = 7 * 2 \text{ Kbps} = 14 \text{ Kbps}$$

Tráfico de Correo electrónico:

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ email}$$

$$C_{Email} = 7 * 0,1 * 48\ Kbps = 33,60\ Kbps$$

Descarga de Archivos:

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ descarga\ archivo}$$

$$C_{Descargar} = 12 * 0,1 * 40\ Kbps = 28\ Kbps$$

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 67,20\ Kbps + 14\ Kbps + 33,60\ Kbps + 28\ Kbps$$

$$C_T = 142,80\ Kbps * 1,25 = 178,50\ Kbps$$

3.5.1.2 Sucursales de Guayaquil

Tecnomega tiene dos sucursales en Guayaquil la más grande y donde se encuentran mayor cantidad de técnicos es la Sucursal Mayor, por lo tanto se instalará el servicio de *Internet* para Guayaquil en esta sucursal.

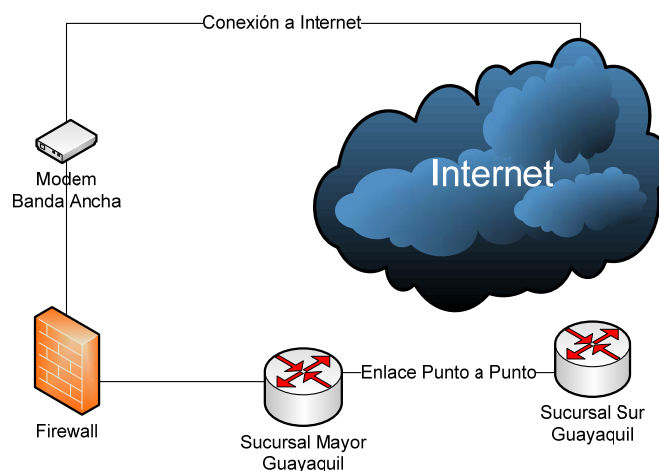


Figura 3-30: Esquema de Conexión a Internet en Guayaquil

Sucursales de Guayaquil			
Sucursal	# Personas	# Personas con acceso a <i>Internet</i>	Capacidad requerida
Mayor	23	16	408,00 Kbps
Sur	9	6	153,00 Kbps
TOTAL	32	22	561,00 Kbps

Tabla 3-63: Cálculo de la Capacidad *Internet* en Guayaquil

$$Capacidad_{Total} = Capacidad_{Sucursales} + Capacidad_{Videoconferencia}$$

$$Capacidad_{Total} = 561 \text{ Kbps} + 240 \text{ Kbps} = 801 \text{ Kbps}$$

$$Capacidad_{Necesaria} = Capacidad_{Total} * 1,1$$

$$Capacidad_{Necesaria} = 801 \text{ Kbps} * 1,1 = 881,1 \text{ Kbps}$$

La capacidad total aproximado es 1 *Mbps*, para 22 usuarios de las dos sucursales de Guayaquil que tienen acceso a *Internet*.

3.5.1.2.1 Sucursal Mayor

Los usuarios de la Sucursal Mayor que utilizan *Internet* son:

Sucursal Mayor Guayaquil			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	3	Si	3
Ventas	7	Si	7
Mercadeo	2	Si	2
Caja	2	No	0
Contabilidad	1	No	0
Crédito	1	Si	1
Bodega	4	No	0
Técnico	3	Si	3
TOTAL	23		16

Tabla 3-64: Acceso a *Internet* Sucursal Mayor Guayaquil

En esta sucursal se tiene un total de 16 usuarios que utilizan *Internet*; las principales aplicaciones que le dan a este servicio son:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{Navegar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ página web}}$$

$$C_{Navegar} = 16 * 0,15 * 64 \text{ Kbps} = 153,60 \text{ Kbps}$$

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM \text{ usuario}}$$

$$C_{IM} = 16 * 2 \text{ Kbps} = 32 \text{ Kbps}$$

Tráfico de Correo electrónico:

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ email}}$$

$$C_{Email} = 16 * 0,1 * 48 \text{ Kbps} = 76,80 \text{ Kbps}$$

Descarga de Archivos:

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ descarga archivo}}$$

$$C_{Descargar} = 16 * 0,1 * 40 \text{ Kbps} = 64 \text{ Kbps}$$

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 153,60 \text{ Kbps} + 32 \text{ Kbps} + 76,80 \text{ Kbps} + 64 \text{ Kbps}$$

$$C_T = 326,40 \text{ Kbps} * 1,25 = 408,00 \text{ Kbps}$$

3.5.1.2.2 Sucursal Sur

Los usuarios de la Sucursal Sur de Guayaquil que utilizan *Internet* son:

Sucursal Sur de Guayaquil			
Departamento	# Personas	Acceso a <i>Internet</i>	# Personas con Acceso a <i>Internet</i>
Administrativo	2	Si	2
Ventas	3	Si	3
Caja	1	No	0
Bodega	2	No	0
Técnico	1	Si	1
TOTAL	9		6

Tabla 3-65: Acceso a *Internet* de la Sucursal Sur Guayaquil

En esta sucursal se tiene un total de 6 usuarios que utilizan *Internet*; las principales aplicaciones que le dan a este servicio son:

- Navegar por sitios *web*
- Mensajería Instantánea
- Correo Electrónico
- Descarga de Archivos

Tráfico de Navegar por sitios *web*:

$$C_{Navegar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ página web}}$$

$$C_{Navegar} = 6 * 0,15 * 64 \text{ Kbps} = 57,60 \text{ Kbps}$$

Tráfico de Mensajería Instantánea:

$$C_{IM} = \#_{usuarios} * C_{IM \text{ usuario}}$$

$$C_{IM} = 6 * 2 \text{ Kbps} = 12 \text{ Kbps}$$

Tráfico de Correo electrónico:

$$C_{Email} = \#_{usuarios} * I_{simultaneidad} * C_{usuario \text{ email}}$$

$$C_{Email} = 6 * 0,1 * 48 \text{ Kbps} = 28,80 \text{ Kbps}$$

Descarga de Archivos:

$$C_{Descargar} = \#_{usuarios} * I_{simultaneidad} * C_{usuario\ descarga\ archivo}$$

$$C_{Descargar} = 6 * 0,1 * 40\ Kbps = 24\ Kbps$$

Capacidad Total:

$$C_T = C_{Navegar} + C_{IM} + C_{email} + C_{Descargar}$$

$$C_T = 57,60\ Kbps + 12\ Kbps + 28,80\ Kbps + 24\ Kbps$$

$$C_T = 122,40\ Kbps * 1,25 = 153,00\ Kbps$$

3.5.2 CÁLCULO DE ENLACES ENTRE SUCURSALES

Los enlaces entre las sucursales son utilizados para:

- Recopilación de Información de las bases de datos para actualización de las aplicaciones de la *Intranet*
- Consultas de inventario en las demás sucursales de la empresa
- Administración remota de equipos de conectividad y servidores
- Ejecutar el *software* de administración de la red.
- Compartir conexiones de *Internet*
- Telefonía y Videoconferencia *IP*

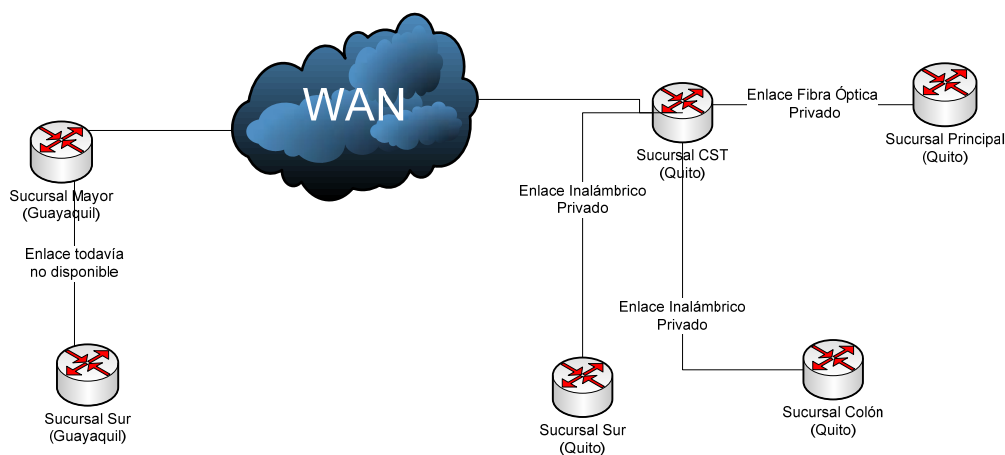


Figura 3-31: Esquema Red WAN de Tecnomega

Overhead Ethernet en Bytes:

$$\begin{aligned}
 O_{Ethernet \text{ sin VLAN}} &= 12_{\text{espacio}} + 8_{\text{preámbulo}} + 14_{\text{encabezado}} + 4_{\text{trailer}} \\
 O_{Ethernet \text{ sin VLAN}} &= 38 \text{ Bytes} \\
 O_{Ethernet \text{ con VLAN}} &= 12_{\text{espacio}} + 8_{\text{preámbulo}} + 18_{\text{encabezado}} + 4_{\text{trailer}} \\
 O_{Ethernet \text{ con VLAN}} &= 42 \text{ Bytes}
 \end{aligned}$$

TCP sobre Ethernet:

Encabezado *IP* = 20 Bytes

Encabezado *TCP* = 20 Bytes

$$\begin{aligned}
 \%Overhead \text{ sin VLAN} &= 100\% - \left(\frac{MTU_{Ethernet} - (E_{IP} - E_{TCP})}{O_{Ethernet \text{ sin VLAN}} + MTU_{Ethernet}} * 100\% \right) \\
 \%Overhead \text{ sin VLAN} &= 100\% - \left(\frac{1500 - 40}{38 + 1500} * 100\% \right) = 5,07\%
 \end{aligned}$$

$$\begin{aligned}
 \%Overhead \text{ con VLAN} &= 100\% - \left(\frac{MTU_{Ethernet} - (E_{IP} - E_{TCP})}{O_{Ethernet \text{ con VLAN}} + MTU_{Ethernet}} * 100\% \right) \\
 \%Overhead \text{ con VLAN} &= 100\% - \left(\frac{1500 - 40}{42 + 1500} * 100\% \right) = 5,32\%
 \end{aligned}$$

Se toma como dato para los enlaces entre sucursales que trabaja con tecnología *Ethernet* el 5% de *Overhead* y para los enlaces *WAN* un 25% de *overhead*, con el respaldo obtenido en los cálculos anteriores.

3.5.2.1 Enlaces Sucursales Quito

La configuración de los enlaces entre las Sucursales de Quito, incluyendo los ruteadores que se requiere para la reingeniería de la red se muestra en la Figura 3-32.

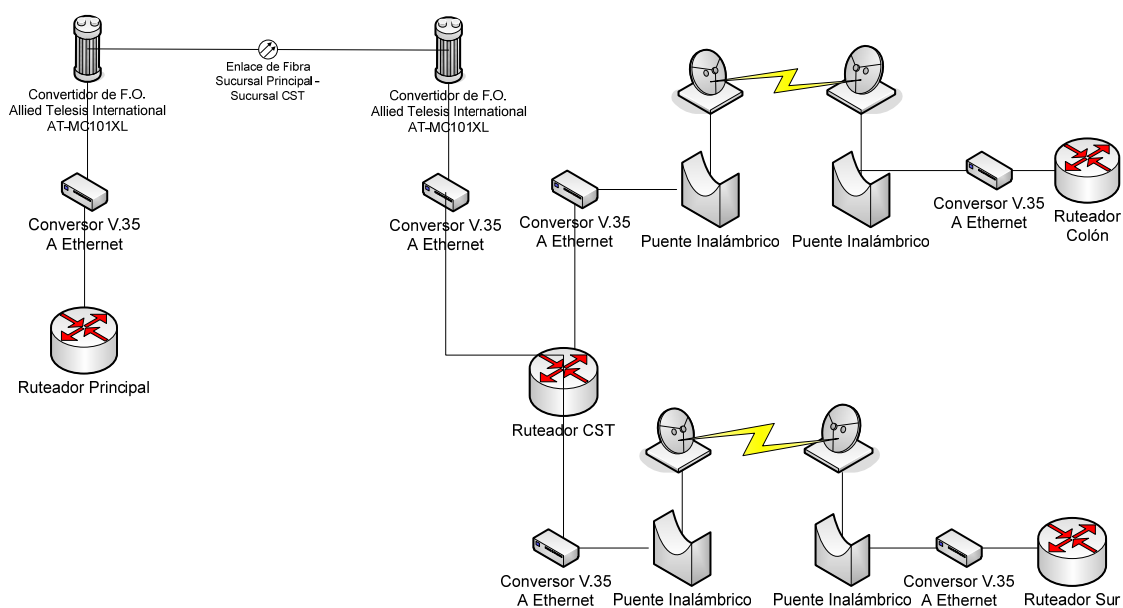


Figura 3-32: Equipos de Conectividad Enlaces Quito

3.5.2.1.1 Enlace Sucursal Principal – CST

Este enlace servirá para:

- Consultas de *stock* en otras sucursales del Sistema *Global Commerce*.
- Actualización de la *Intranet* con las bases de datos de las sucursales.
- La salida de Quito hacia *Internet* estará en la sucursal CST; el uso de Internet de la Sucursal Principal se enrutará por este enlace hacia el ruteador de la sucursal CST.
- Telefonía *IP* entre las sucursales y fuera de ellas.
- Videoconferencia *IP* entre sucursales y fuera de ellas

Consulta de *Stock* de otra sucursal:

$$C_{\text{consulta Global Commerce}} = T_{\text{consulta}} * t_{\text{carga}}$$

$$C_{\text{consulta Global Commerce}} = 2 \frac{KB}{\text{consulta}} * \frac{1 \text{ consulta}}{1 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 16 \text{ Kbps}$$

$$C_{\text{consulta}} = \#_{\text{usuarios}} * I_{\text{simultaneidad}} * C_{\text{consulta Global Commerce}}$$

$$C_{\text{consulta}} = 39 * 0,1 * 16 \text{ Kbps} = 62,40 \text{ Kbps}$$

El manual de *Global Commerce* indica que cada consulta realizada genera una tabla temporal de 2 KB, esto debe ser transmitido en un segundo o el sistema lanzará un mensaje de error suponiendo que la conexión a la base de datos se ha perdido. Se asume una simultaneidad del 10% en consultas.

Réplica de Bases de Datos³⁷:

$$T_{Base\ de\ Datos} = 100\ KB$$

$$C_{Réplica\ Base\ de\ Datos} = \frac{T_{Base\ de\ Datos}}{t_{réplica}}$$

$$C_{Réplica\ Base\ de\ Datos} = \frac{100\ KB}{60s} * \frac{8\ bits}{1\ Byte} = 13,33\ Kbps$$

Se asume que una base de datos de 100 KB se replique en 60 s que es un tiempo aceptable, lo cual espera el Administrador de la Red.

Internet:

$$C_{Internet\ Sucursal\ Principal} = 713,75\ Kbps$$

Telefonía IP:

$$C_{Telefonía\ IP} = 374,40\ Kbps$$

Videoconferencia IP:

$$C_{videoconferencia\ IP} = 192,00\ Kbps$$

³⁷ Las réplicas de la base de datos no se realizan todo el tiempo, se realizan una vez al día a las 2 pm que es la hora donde menos se utiliza la red, según el Administrador de la misma.

Capacidad Total:

$$C_{Total} = C_{Consultas Stock} + C_{Réplica Base de Datos} + C_{Internet} + C_{Telefonía IP} \\ + C_{Videoconferencia IP}$$

$$C_{Total} = 44,8 Kbps + 13,33 Kbps + 713,75 Kbps + 374,40 Kbps + 192 Kbps$$

$$C_{Total} = 1338,28 Kbps * 1,05^{38} = 1405,19 Kbps$$

Capacidad más el 10% de tolerancia

$$C_{Necesario} = 1405,19 Kbps * 1,1 = 1545,71 Kbps$$

La capacidad necesaria para el enlace entre las sucursales Principal – CST es de 1,5 Mbps aproximadamente; el enlace físico con el que se cuenta al momento es de 100 Mbps. En este enlace se pueden utilizar las aplicaciones anteriormente detalladas.

3.5.2.1.2 Enlace Sucursal CST – Colón

Este enlace servirá para:

- Consultas de *stock* en otras sucursales del Sistema *Global Commerce*.
- Actualización de la *Intranet* por medio de las bases de datos de las sucursales.
- La salida de Quito hacia *Internet* estará en la sucursal CST; el uso de *Internet* de la Sucursal Colón se enrutará por este enlace hacia el ruteador de la sucursal CST.
- Telefonía y Videoconferencia *IP* entre las sucursales y fuera de ellas.

³⁸ Se asume que el *overhead* promedio es 5% de una red *WAN*, como: *ATM* o *Frame Relay*.

Consulta de Stock de otra sucursal:

$$C_{\text{consulta Global Commerce}} = T_{\text{consulta}} * t_{\text{carga}}$$

$$C_{\text{consulta Global Commerce}} = 2 \frac{KB}{\text{consulta}} * \frac{1 \text{ consulta}}{1 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 16 \text{ Kbps}$$

$$C_{\text{consulta}} = \#_{\text{usuarios}} * I_{\text{simultaneidad}} * C_{\text{consulta Global Commerce}}$$

$$C_{\text{consulta}} = 17 * 0,1 * 16 \text{ Kbps} = 27,20 \text{ Kbps}$$

Réplica de Bases de Datos:

$$T_{\text{Base de Datos}} = 100 \text{ KB}$$

$$C_{\text{Réplica Base de Datos}} = \frac{T_{\text{Base de Datos}}}{t_{\text{réplica}}}$$

$$C_{\text{Réplica Base de Datos}} = \frac{100 \text{ KB}}{60s} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 13,33 \text{ Kbps}$$

Internet:

$$C_{\text{Internet Sucursal Colón}} = 306 \text{ Kbps}$$

Telefonía IP:

$$C_{\text{Telefonía IP}} = 249,60 \text{ Kbps}$$

Videoconferencia IP:

$$C_{\text{videoconferencia IP}} = 192,00 \text{ Kbps}$$

Capacidad Total:

$$C_{\text{Total}} = C_{\text{Stock}} + C_{\text{Base de Datos}} + C_{\text{Internet}} + C_{\text{Telefonía IP}} + C_{\text{Videoconferencia IP}}$$

$$C_{\text{Total}} = 27,20 \text{ Kbps} + 13,33 \text{ Kbps} + 306 \text{ Kbps} + 249,60 \text{ Kbps} + 192 \text{ Kbps}$$

$$C_{\text{Total}} = 787,91 \text{ Kbps} * 1,05 = 827,31 \text{ Kbps}$$

La tolerancia será el 10% para el diseño de este enlace

$$C_{Necesario} = 827,31 \text{ Kbps} * 1,1 = 910,04 \text{ Kbps}$$

La capacidad necesaria para el enlace entre las sucursales Colón – CST es de 1 Mbps aproximadamente, el enlace con el que se cuenta es de 5.5 Mbps. En este enlace se pueden utilizar las aplicaciones anteriormente detalladas.

3.5.2.1.3 Enlace Sucursal CST – Sur

Este enlace servirá para:

- Consultas de *stock* en otras sucursales del Sistema *Global Commerce*.
- Actualización del *SIAC* mediante las bases de datos de las sucursales.
- La salida de Quito hacia *Internet* estará en la sucursal CST; el uso de *Internet* de la Sucursal Sur se enrutará por este enlace hacia el ruteador de la sucursal CST.
- Telefonía *IP* entre las sucursales y fuera de ellas.
- Videoconferencia *IP* entre las sucursales y fuera de ellas.

Consulta de *Stock* de otra sucursal:

$$C_{\text{consulta Global Commerce}} = T_{\text{consulta}} * t_{\text{carga}}$$

$$C_{\text{consulta Global Commerce}} = 2 \frac{KB}{\text{consulta}} * \frac{1 \text{ consulta}}{1 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 16 \text{ Kbps}$$

$$C_{\text{consulta}} = \#_{\text{usuarios}} * I_{\text{simultaneidad}} * C_{\text{consulta Global Commerce}}$$

$$C_{\text{consulta}} = 11 * 0,1 * 16 \text{ Kbps} = 17,60 \text{ Kbps}$$

Réplica de Bases de Datos:

$$T_{\text{Base de Datos}} = 100 \text{ KB}$$

$$C_{\text{Réplica Base de Datos}} = \frac{T_{\text{Base de Datos}}}{t_{\text{réplica}}}$$

$$C_{\text{Réplica Base de Datos}} = \frac{100 \text{ KB}}{60s} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 13,33 \text{ Kbps}$$

Internet:

$$C_{Internet\ Sucursal\ Sur\ Quito} = 178,50\ Kbps$$

Telefonía IP:

$$C_{Telefonía\ IP} = 124,80\ Kbps$$

Videoconferencia IP:

$$C_{Videoconferencia\ IP} = 192\ Kbps$$

Capacidad Total:

$$C_{Total} = C_{Consultas\ Stock} + C_{Réplica\ Base\ de\ Datos} + C_{Internet} + C_{Telefonía\ IP} \\ + C_{Videoconferencia\ IP}$$

$$C_{Total} = 17,60\ Kbps + 13,33\ Kbps + 178,50\ Kbps + 124,80\ Kbps + 192\ Kbps$$

$$C_{Total} = 526,20\ Kbps * 1,05 = 552,51\ Kbps$$

La tolerancia para este enlace es del 10%

$$C_{Necesario} = 552,51\ Kbps * 1,1 = 607,76\ Kbps$$

La capacidad necesaria para el enlace entre las sucursales CST - Sur es de 608 Kbps aproximadamente, el enlace con el que se cuenta al momento es de 1 Mbps. En este enlace se pueden utilizar las aplicaciones anteriormente detalladas sin tener problemas de saturación del canal.

3.5.2.2 Enlace Quito – Guayaquil

El enlace entre Quito y Guayaquil debe ser un enlace arrendado para datos que garantice la capacidad fruto de los cálculos que se van a realizar, para asegurar servicios críticos como la Telefonía *IP*.

La tecnología manejada en este enlace se escogerá en el Capítulo 4, donde se presentarán las opciones y sus respectivos precios. Las opciones tendrán que detallar características como: disponibilidad, tipo de red, soporte, etc.

3.5.2.2.1 Enlace Sucursal CST (Quito) – Mayor (Guayaquil)

El Enlace Quito – Guayaquil se utilizará principalmente para:

- Consulta de *Stock* entre las Sucursales
- Réplica de Bases de Datos
- Telefonía *IP* entre Sucursales de Quito y Guayaquil

Consulta de *Stock* entre sucursales:

$$C_{\text{consulta Global Commerce}} = T_{\text{consulta}} * t_{\text{carga}}$$

$$C_{\text{consulta Global Commerce}} = 2 \frac{KB}{\text{consulta}} * \frac{1 \text{ consulta}}{1 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 16 \text{ Kbps}$$

Este enlace transportará las consultas de *stock* entre las sucursales de Quito y Guayaquil; éstas no son tan frecuentes como las consultas entre las sucursales de la misma ciudad usadas para transferencias de mercadería. Se asumirá un Índice de simultaneidad del 4% para esquematizar su frecuencia, ya que esta consulta se realiza solo cuando el *stock* de una ciudad se terminó y se necesita hacer una transferencia entre ciudades.

$$C_{\text{consulta}} = \#_{\text{usuarios}} * I_{\text{simultaneidad}} * C_{\text{consulta Global Commerce}}$$

$$C_{\text{consulta}} = 90 * 0,04 * 16 \text{ Kbps} = 57,60 \text{ Kbps}$$

Réplica de Bases de Datos:

$$T_{Base\ de\ Datos} = 100\ KB$$

$$C_{Réplica\ Base\ de\ Datos} = \#Bases\ de\ Datos * \frac{T_{Base\ de\ Datos}}{t_{réplica}}$$

$$C_{Réplica\ Base\ de\ Datos} = 1 * \frac{100\ KB}{60s} * \frac{8\ bits}{1\ Byte} = 13,33\ Kbps$$

Telefonía IP:

$$C_{Telefonía\ IP\ Quito-Guayaquil} = 211,20\ Kbps$$

Capacidad Total:

$$C_{Total} = C_{Consultas\ Stock} + C_{Réplica\ Base\ de\ Datos} + C_{Telefonía\ IP} + C_{Videoconferencia}$$

$$C_{Total} = 57,60\ Kbps + 13,33\ Kbps + 148,80\ Kbps + 192\ Kbps$$

$$C_{Total} = 474,13\ Kbps * 1,25 = 592,66\ Kbps$$

La tolerancia para este enlace será del 10%:

$$C_{Necesario} = 592,66\ Kbps * 1,1 = 651,93\ Kbps$$

De acuerdo a los cálculos, el enlace debe garantizar 512 Kbps y se puede contratar una capacidad en exceso (EIR³⁹) de 128 Kbps, para datos entre Guayaquil y Quito. La tecnología del mismo se debe escoger en el Capítulo 4 donde se detallarán las opciones disponibles y sus costos.

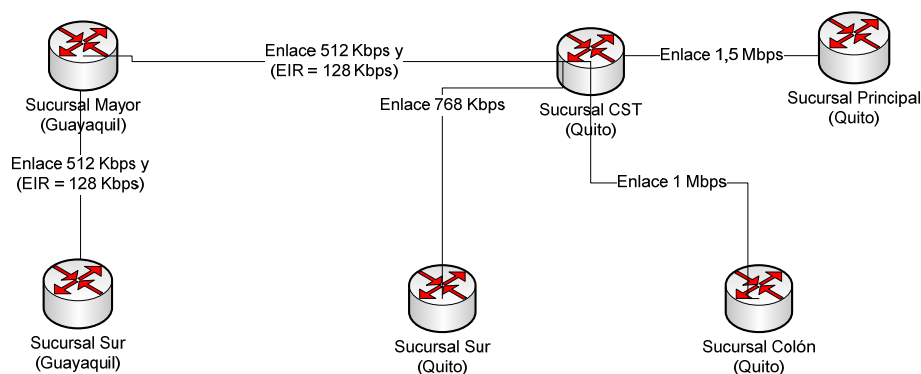


Figura 3-33: Capacidad de los Enlaces entre Sucursales

³⁹ EIR (Excess Information Rate)

3.5.2.3 Enlaces Guayaquil

Los enlaces entre las sucursales de Guayaquil se sugiere que sean arrendados, por eso se detallarán las características necesarias. Al contratar un enlace se garantiza una alta disponibilidad y la empresa puede realizar mejor sus actividades normales.

3.5.2.3.1 Enlace Sucursal Mayor – Sur

Este enlace servirá para:

- Consultas de *stock* en otras sucursales del Sistema *Global Commerce*.
- Actualización de la *Intranet* por medio de las bases de datos de las sucursales.
- La salida hacia *Internet*.
- Telefonía y Videoconferencia *IP* entre las sucursales y fuera de ellas.

Consulta de *Stock* de otra sucursal:

$$C_{\text{consulta Global Commerce}} = T_{\text{consulta}} * t_{\text{carga}}$$

$$C_{\text{consulta Global Commerce}} = 2 \frac{KB}{\text{consulta}} * \frac{1 \text{ consulta}}{1 \text{ segundos}} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 16 \text{ Kbps}$$

$$C_{\text{consulta}} = \#_{\text{usuarios}} * I_{\text{simultaneidad}} * C_{\text{consulta Global Commerce}}$$

$$C_{\text{consulta}} = 9 * 0,1 * 16 \text{ Kbps} = 14,40 \text{ Kbps}$$

Réplica de Bases de Datos:

$$T_{\text{Base de Datos}} = 100 \text{ KB}$$

$$AB_{\text{Réplica Base de Datos}} = \frac{T_{\text{Base de Datos}}}{t_{\text{réplica}}}$$

$$AB_{\text{Réplica Base de Datos}} = \frac{100 \text{ KB}}{60s} * \frac{8 \text{ bits}}{1 \text{ Byte}} = 13,33 \text{ Kbps}$$

Internet:

$$C_{Internet\ Sucursal\ Sur\ de\ Guayaquil} = 153\ Kbps$$

Telefonía IP:

$$C_{Telefonía\ IP\ Sucursal\ Sur\ de\ Guayaquil} = 105,60\ Kbps$$

Videoconferencia IP:

$$C_{Videoconferencia\ IP} = 192\ Kbps$$

Capacidad Total:

$$C_{Total} = C_{Consultas\ Stock} + C_{Replica\ Base\ de\ Datos} + C_{Internet} + C_{Telefonía\ IP} + C_{Videoconferencia\ IP}$$

$$C_{Total} = 14,40\ Kbps + 13,33\ Kbps + 153\ Kbps + 74,40\ Kbps + 192\ Kbps$$

$$C_{Total} = 459,73\ Kbps * 1,25 = 574,66\ Kbps$$

La tolerancia para este enlace será del 10%

$$C_{Total} = 574,66\ Kbps * 1,1 = 632,13\ Kbps$$

Teniendo en cuenta que la réplica de la base de datos no se realiza todo el tiempo sino cuando menos tráfico se tiene en la red, se sugiere contratar una capacidad de 512 Kbps con un exceso de 128 Kbps para incluir en esto la tolerancia o capacidad extra requerida en casos de alta demanda.

3.6 SEGURIDAD DE LA RED

3.6.1 SEGURIDAD FÍSICA

La seguridad física de la red está relacionada con la pérdida o robos de equipos y/o información de la empresa. Estos robos pueden ocasionar interrupción de las actividades de la empresa, por esto se especifican las medidas de seguridad que se deben tomar para prevenir estas situaciones.

La seguridad física de la red recae principalmente en:

- Seguridad de los equipos
- Seguridad de los respaldos de información organizacional

3.6.1.1 Seguridad de Equipos

Todas las sucursales de Tecnomega tienen guardianía privada para proteger los bienes de la empresa y la mercadería que comercializa. Esto es una gran ventaja para la seguridad física de la red, ya que se resguardan los equipos de conectividad y computación contra robos.

La seguridad de los equipos de Conectividad es muy importante, por ejemplo, si no se tienen cuartos de telecomunicaciones cualquier persona desconecta un cable intencional o inintencionalmente y se pierde la conectividad con una estación de trabajo o un servidor. El Departamento de Sistemas tendrá que encontrar el fallo, perdiendo tiempo y dinero.

Para que no ocurran este tipo de cosas se sugiere construir cuartos de telecomunicaciones, donde no existan. Estos cuartos deberán disponer de: sistemas de control de accesos, normas eléctricas, control de temperatura y control contra incendios para no tener interrupción de operaciones.

Por la falta de cuartos de telecomunicaciones con control de accesos se dan robos de información conectando un computador que tiene instalado un *sniffer* en el *switch* y roba toda la información, con la facilidad que no está encriptada la información y no se tienen restricciones de acceso a la red.

En la Sucursal Principal que es la más antigua, no se tiene un cuarto de telecomunicaciones y los equipos de conectividad se encuentran en un lugar accesible a empleados y clientes. Como prioridad para el cumplimiento de un sistema de seguridad se debe reubicar este *rack* con los equipos, en un lugar con acceso restringido y que cumpla con los requerimientos para instalar un cuarto de telecomunicaciones.

Otra sucursal que no tiene un cuarto de telecomunicaciones es la Sucursal CST, donde se tienen distribuidos los equipos de conectividad en tres partes del edificio, lo que dificulta su administración y seguridad. En esta sucursal también se debe implementar un cuarto de telecomunicaciones centralizado para ubicar los equipos; no hace falta más de un cuarto de telecomunicaciones porque la sucursal tiene dos pisos y no es tan grande como para hacer un cuarto de telecomunicaciones en cada piso.

Las demás sucursales tienen un cuarto de telecomunicaciones que se diseñó para ello, y también el cableado estructurado se diseñó a la par. Se debería revisar que estos cuartos de telecomunicaciones cumplan con los estándares y normas que los rigen, pero esto no está dentro del alcance de este proyecto de titulación.

3.6.1.2 Seguridad del Respaldo de Información

Los discos o las cintas de respaldo de información deben ser manejados con la mayor cautela, muchas veces se cumple con respaldar la información de los servidores y/o otra información importante para la empresa y no se tiene procesos para la seguridad física de estos respaldos.

Los respaldos de información de cada sucursal deben tener dos o tres copias, una debe ser guardada en una caja fuerte ubicada en el cuarto de telecomunicaciones de la sucursal y la o las dos copias restantes en los cuartos de telecomunicaciones de las otras sucursales de la misma ciudad, para que esté a la mano solamente del personal autorizado.

Los respaldos de información tienen un tiempo de vigencia, los que ya no se necesiten deben ser totalmente destruidos para prevenir que al desecharlos exista algún tipo de robo de información; ésta es una parte importante del procedimiento para la seguridad de los respaldos de información.

3.6.2 SEGURIDAD LÓGICA

La seguridad lógica de la red se logra por medio de: *firewalls*, *IPS*, *IDS*, esquemas de seguridad inalámbrica, creación de un dominio de la empresa para autenticación y autorización de usuarios, etc. Estas medidas de seguridad protegen la información que es el principal activo de la empresa.

La información organizacional es uno de los principales activos de la empresa, ya que sin ella no se puede trabajar. Por ejemplo si se pierden las cuentas por cobrar, existirán serios problemas económicos, por lo tanto se debe cuidar la información con los medios que estén a nuestro alcance.

El cambio de contraseñas para acceso a la red y al dominio de la empresa será mensual, en todos los servidores de dominio se incluirá la política de seguridad de cambio de contraseña mensual obligatoria, sino se cambia de contraseña no se permitirá el acceso.

Si un usuario ingresa erróneamente su contraseña tres veces consecutivas su cuenta será bloqueada por una hora, y en casos de urgencia se deberá pedir al administrador de la red que desbloquee la cuenta.

El administrador de la red también está facultado a bloquear cuentas de usuarios que se encuentre en vacaciones o que ya no trabajen en la empresa, en un plazo máximo de 24 horas después de recibir la notificación del Departamento de Recursos Humanos.

Para el acceso remoto se tiene que registrar el usuario con la misma contraseña del dominio de la empresa; la autenticación de acceso remoto se lo realizará por medio del servidor *RADIUS* implementado con el servicio *IAS* y con el esquema de autenticación *PEAP –MS-CHAPv2*

3.6.2.1 Autenticación de Usuarios

Aprovechando que la plataforma utilizada en Tecnomega es de *Microsoft*, se implementarán las seguridades de la red inalámbrica con ayuda de los servidores de la empresa. *Windows 2003 Server* tiene un servicio llamado Servicio de Autenticación de *Internet (IAS)* que se puede utilizar como servidor *RADIUS* para la autenticación, autorización y administración de cuentas de clientes *RADIUS*. Es decir tiene algunas funciones de administración de conexiones por *Internet*, tales como: Servidor de Acceso Telefónico, Servidor *VPN* y Punto de Acceso Inalámbrico.

El uso que se le dará a *IAS* es para la administración de las conexiones inalámbricas, donde se utilizarán seguridades de acceso por medio de contraseñas y certificados digitales utilizando *PEAP-EAP-MS-CHAPv2* que da al usuario una mayor facilidad de uso sin disminuir considerablemente la seguridad de la red.

Para la autenticación de credenciales de un usuario que intenta conectarse, *IAS* utiliza un dominio de *Active Directory*, donde se tiene una base de datos de los usuarios registrados y sus contraseñas para que puedan ingresar a la red. Para la autorización de la conexión, *IAS* utiliza las propiedades de marcado de la cuenta de usuario y las directivas de acceso remoto.

IAS soporta 802.1X, éste es un estándar de la *IEEE* para brindar acceso autenticado a redes *Ethernet* por cable y redes inalámbricas 802.11. Por medio de este protocolo se mejora la seguridad de la red y la compatibilidad, incorporando: identificación, autenticación, administración de claves y creación de cuentas de usuarios de forma centralizada.

802.1X ofrece compatibilidad con varios tipos de Protocolo de Autenticación Extensible (*EAP*), los cuales permiten elegir distintos tipos de autenticación para clientes y servidores. 802.1X utiliza *EAP* para intercambiar mensajes durante el proceso de autenticación, *EAP* utiliza métodos de autenticación arbitrarios, tales como: certificados, tarjetas inteligentes o credenciales.

EAP permite establecer comunicaciones abiertas entre clientes *EAP*, en este caso entre el cliente, y los servidores *EAP*. La conversación se compone de requerimientos del servidor y respuestas a los requerimientos por parte del cliente a ser autenticado.

Microsoft es compatible con dos tipos de protocolos *EAP*, que son:

- *EAP-TLS*, trabaja con la seguridad en la capa de transporte, en entornos basados en certificados digitales en el cliente y el servidor, razón por la cual se dificulta su implementación y se incrementan costos, pero es el protocolo más seguro.
- *EAP-MS-CHAPv2*, es un método de autenticación mutuo que permite autenticar equipos y usuarios por medio de contraseñas; el servidor debe tener instalado un certificado digital para autenticarlo, si es un servidor seguro. Este método es más simple de implementar y mucho más barato, pero no es tan seguro como el anterior.

EAP-MS-CHAPv2 funciona solo con *PEAP* (Protocolo de Autenticación Extensible Protegido) que utiliza seguridad de nivel de transporte *TLS*, crea un canal cifrado para proteger los métodos de autenticación *EAP*. Esto da mayor seguridad para el intercambio de claves dinámicas y el proceso

autenticación, adicionalmente ofrece reconexión rápida en caso de que el cliente inalámbrico se esté moviendo entre puntos inalámbricos, su clave de acceso se guarda en cache y no es solicitada nuevamente.

Por facilidad de uso y sin sacrificar la seguridad de la red se escogió el Protocolo *PEAP-EAP-MS-CHAPv2*, ya que un usuario para conectarse a la red necesita estar registrado en el dominio, tener su nombre de usuario y contraseña. El nivel de seguridad es bastante aceptable, por esta razón fue escogido como esquema de seguridad para la red.

En la otra opción de *EAP-TLS* se tienen que instalar certificados digitales en cada uno de los clientes inalámbricos y en el servidor para poder acceder a la red inalámbrica. Teniendo en cuenta los costos de los certificados digitales y que éstos tienen un tiempo de validez, esta solución es muy difícil de implementar y costosa.

Otra razón por haber escogido este servicio *IAS* de *Microsoft* como servidor *RADIUS*, es que está disponible en todas las versiones de *Windows 2003 Server*; dependiendo de la versión tiene restricciones como:

- *Windows 2003 Server* Edición Estándar puede tener 50 clientes *RADIUS* y dos grupos de servidores *RADIUS* remotos.
- *Windows 2003 Server* Edición *Enterprise* y Edición *Data Center* puede manejar un número ilimitado de clientes *RADIUS* y grupos de servidores remotos.

Al escoger este servidor *RADIUS* de *Windows* se disminuyen costos y se tiene una aplicación con soporte de *Microsoft* que es totalmente compatible con el Sistema Operativo, que se está usando. Además, está totalmente integrada con *Windows 2003 Server* y maneja esquemas de seguridad estándar, fácilmente configurables en los clientes que tienen instalado Sistemas Operativos de *Microsoft*, como: *Windows XP Profesional SP2*, *Windows Vista Business* y *Ultimate*.

Windows XP Profesional SP2, Windows Vista Bussiness, Windows Vista Ultimate son los sistemas operativos de *Microsoft* para empresas; éstos se pueden conectar a un dominio, lo cual es muy importante para este esquema de seguridad porque está integrado con el dominio de la empresa y son los únicos sistemas operativos que tienen este tipo de seguridades.

Existen programas que ayudan a la administración de autenticación de usuarios, que se integran con la mayoría de servidores *RADIUS* y dominios de *Active Directory* en el caso de *Microsoft*, facilitan la administración integral de *switches* y sus puertos relacionándolos con los usuarios, estableciendo si un puerto es para varios usuarios o solo para uno, etc. Estos programas son:

- *Cisco Secure ACS*
- *3COM Network Access Manager*

3.6.2.2 Seguridad Red Cableada

En cada una de las sucursales se instalarán equipos de seguridad unificada, que cumplen funciones de:

- Sistema de Prevención de Intrusos: analiza el tráfico tanto de *Internet* como de la *Intranet*, protegiendo a la red contra amenazas y ayuda a impedir el *hacking* de capacidad de transmisión y tráfico malicioso, tales como: espías, gusanos virus, troyanos, intentos de estafas, amenazas de *VoIP* y *antispam*. Equipos de este tipo son: *3COM Sistema de Seguridad Unificada X5* y *Cisco ASA 5510*.
- Soporte *VPN* Avanzado: por una *VPN* se pueden transmitir software malicioso, el sistema monitorea el túnel *VPN* en dos direcciones para mitigar ataques en estos túneles *VPN*.
- Bloqueo de Aplicaciones y filtro de contenidos *web*: bloquean aplicaciones *P2P* para optimizar el uso de la capacidad de *Internet*. El filtro de contenidos restringe sitios *web* que no deben ser visitados por los empleados, éstos están registrados en una base de datos.

- **Firewall:** analiza los paquetes que pasan a través suyo para no permitir el paso de paquetes maliciosos que comprometan a la red. El *firewall* puede bloquear puertos para que los paquetes pasen solo por los puertos permitidos y también se pueden configurar bloqueos por *VLANs*, rango de direcciones *IP* y una dirección *IP*. Esta herramienta puede ser utilizada para bloquear los puertos *HTTP*, *SMTP*, etc., a los usuarios que no deban tener acceso a ellos.

3.6.2.2.1 VPNs entre Sucursales

Las *VPNs* se levantarán en los enlaces entre las sucursales sean éstos privados o arrendados para garantizar la integridad y confidencialidad de la información transmitida. Las *VPNs* se implementarán en la capa de red para tener mayor seguridad que en las capas superiores, utilizando el protocolo *IPSec* que es muy utilizado en *VPNs*.

Los equipos que levantarán y terminarán las *VPNs* serán los *firewalls* o equipos de seguridad unificada que tienen un manejo de *VPNs* avanzado para poder monitorearlas y eliminar todo tipo de *malware* que pueda existir.

En la Figura 3-34 se presenta un esquema de las *VPNs* entre las sucursales.

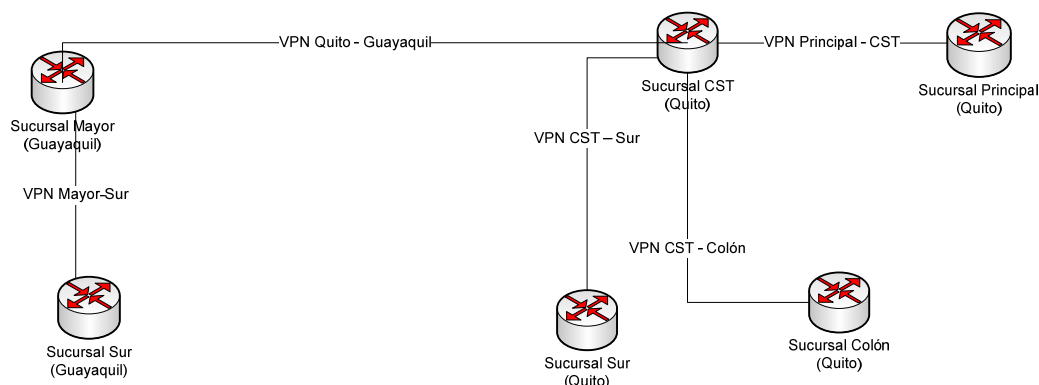


Figura 3-34: VPNs Sucursales

3.6.2.2.2 Bloqueo de Puertos en el Firewall

Los *firewalls* deben cerrar todos los puertos que no sean utilizados y por medio de un *IPS* deben ser monitoreados para no tener ataques por los puertos abiertos. A continuación se detallan los puertos que se deben bloquear para toda la red.

Puertos de Inicio de Sesión:

# puerto	Protocolo Capa Aplicación	Protocolo Capa Transporte
23	<i>Telnet</i>	<i>TCP</i>
22	<i>SSH</i>	<i>TCP</i>
21	<i>FTP</i>	<i>TCP</i>
139	<i>NetBios</i>	<i>TCP</i>
512 - 514	<i>RLOGIN</i>	<i>TCP</i>

Tabla 3-66: Puertos a bloquear de Inicio de Sesión

Para Computadores con *Linux*, protección *RPC* y *NFS*:

# puerto	Protocolo Capa Aplicación	Protocolo Capa Transporte
111	<i>Portmap / rpcbind</i>	<i>TCP y UDP</i>
2049	<i>NFS</i>	<i>TCP y UDP</i>
4045	<i>lockd</i>	<i>TCP y UDP</i>

Tabla 3-67: Puertos a bloquear en Servidores o Estaciones de Trabajo *Linux*

Para computadores con *Windows*, protección *NetBios*:

- *Windows 2000*:

# puerto	Protocolo Capa Aplicación	Protocolo Capa Transporte
135	<i>Loc-srv</i>	<i>TCP y UDP</i>
137	<i>Nbname</i>	<i>UDP</i>
138	<i>Nbdatagram</i>	<i>UDP</i>
139	<i>Nbsession</i>	<i>TCP</i>
445	<i>Microsoft-ds</i>	<i>TCP y UDP</i>

Tabla 3-68: Puertos a bloquear en Servidores con *Windows 2000*

- *Windows XP:*

# puerto	Protocolo Capa Aplicación	Protocolo Capa Transporte
6000 - 6255	<i>NetBios</i>	<i>TCP y UDP</i>

Tabla 3-69: Puertos a bloquear en Estaciones de Trabajo con *Windows XP*

Servicio de Nombres (*DNS*)⁴⁰:

# puertos	Protocolo Capa Aplicación	Protocolo Capa Transporte
53	<i>DNS</i>	<i>UDP</i>
389	<i>LDAP</i>	<i>TCP y UDP</i>

Tabla 3-70: Puertos a bloquear en equipos que no sean Servidores *DNS*

Correo Electrónico⁴¹:

# puertos	Protocolo Capa Aplicación	Protocolo Capa Transporte
25	<i>SMTP</i>	<i>TCP</i>
109 - 110	<i>POP</i>	<i>TCP</i>
143	<i>IMAP</i>	<i>TCP</i>

Tabla 3-71: Puertos a bloquear en equipos que no sean Servidores de Correo

*Web*⁴²:

# puertos	Protocolo Capa Aplicación	Protocolo Capa Transporte
80, 8000, 8080, 8888	<i>HTTP</i>	<i>TCP</i>
443	<i>SSL</i>	<i>TCP</i>

Tabla 3-72: Puertos a bloquear en equipos que no sean Servidores *Web*

⁴⁰ Bloquear los puertos de *DNS* en todos los computadores que no sean servidores *DNS*.

⁴¹ Bloquear los puertos *SMTP*, *POP3* e *IMAP* en computadores que no son Servidores de Correo Electrónico.

⁴² Bloquear los puertos *HTTP* y *SSL* en computadores que no son Servidores *Web*.

Bloquear *ICMP*:

Hay que bloquear los mensajes:

- *Echo Request*
- *Echo Replay*
- Tiempo excedido
- Destino Inalcanzable

Otros puertos para bloquear

# puertos	Protocolo Capa Aplicación	Protocolo Capa Transporte
1-20		<i>TCP y UDP</i>
37	Tiempo	<i>TCP y UDP</i>
69	<i>TFTP</i>	<i>UDP</i>
79	<i>Finger</i>	<i>TCP</i>
119	<i>NNTP</i>	<i>TCP</i>
123	<i>NTP</i>	<i>UDP</i>
515	<i>LPD</i>	<i>TCP</i>
514	<i>Syslog</i>	<i>UDP</i>
179	<i>BGP</i>	<i>TCP</i>
1080	<i>SOCKS</i>	<i>TCP</i>

Tabla 3-73: Puertos Misceláneos para bloquear en el *Firewall*

Se deben bloquear: las direcciones suplantadas, es decir direcciones contenidas en paquetes que llegan desde fuera con direcciones de la red, los que tengan direcciones reservadas por la *IANA*, también los paquetes con rutas predefinidas y los que tengan activadas las opciones de *IP*

3.6.2.2.3 Manejo de Vulnerabilidades

El manejo de vulnerabilidades es muy importante para la seguridad integral de la red; por lo general los ataques son posibles en computadores que no tienen instalados los parches de seguridad que publica el desarrollador del *software*. Los atacantes aprovechan estos huecos de seguridad conocidos, para entrar y hacer daño al sistema.

a) *Vulnerabilidades con Comunidades SNMP por defecto*

Una vulnerabilidad muy peligrosa son los nombres de las comunidades *SNMP* por defecto, ya que el atacante puede tomar control de los equipos de la red solo conociendo el nombre de la comunidad *SNMP*, y si se deja la comunidad por defecto es muy probable que se llegue a consumir el ataque. Esto se da porque *SNMP* hasta la versión 3 no incluye autenticación.

SNMP v1/v2c no provee encriptación por lo que es fácil colocar un *snifer*, capturar el tráfico *SNMP* y darse cuenta de la estructura de la red para poderla atacarla. Por esto es importante la autenticación y autorización de usuarios en la red para complicar conexiones no autorizadas.

Para erradicar esta vulnerabilidad se deben configurar todos los dispositivos que soporten *SNMP* con un nombre de comunidad no tan fácil de suponer y mantenerlo en secreto, para que personas no autorizadas no tengan posibilidad de tomar control de la red por medio de un *NMS* o un *sniffer* y dejar fuera de servicio a un computador o a toda la red.

b) *Manejo de registro de eventos de la red*

El manejo de registro de eventos es muy útil en caso de que un ataque haya ocurrido, con esto se puede saber a ciencia cierta qué efectos tuvo el ataque y qué fue lo afectado, para poder hacer las correcciones del caso.

Los equipos para seguridad de redes como los Sistemas de Seguridad Unificada tienen la característica de llevar registros de los eventos ocurridos en la red, para que conjuntamente con el *IPS* notificar cuándo se tiene un ataque en curso y tomar acciones para truncar el mismo.

Ejemplos de eventos que son importantes para registrar:

- Intento de acceso con una contraseña errónea
- Correcto acceso al sistema
- Anomalías en el funcionamiento del sistema
- Alertas cuando ocurre un evento
- Errores de *hardware* o *software*

3.6.2.3 Seguridad Red Inalámbrica

Los equipos de red inalámbrica brindan seguridades según el nivel que necesite el cliente; por ejemplo, se puede tener acceso a una red inalámbrica sin clave o con seguridad personal, es decir con una contraseña compartida. Pero esto no es suficiente para la red inalámbrica de una empresa que debe ofrecer un esquema de seguridad que integre autenticación del usuario con el servidor de dominio por medio de su nombre de usuario y contraseña.

La seguridad de la red inalámbrica es una parte muy importante para que se haya integrado a la red cableada, porque se ha tenido algunos accesos no autorizados por donde se han sustraído información confidencial.

La red inalámbrica tendrá un esquema de seguridad *WPA2 Enterprise* con encriptación *AES* que es el más robusto al momento. Para la autenticación se utilizará *802.1X* con un servidor *RADIUS* implementado con *IAS* de *Microsoft*.

IAS está totalmente integrado con *Active Directory* y el dominio para la autenticación de usuarios; el usuario que no se autentique correctamente no podrá tener acceso a la red. Este esquema puede manejar algunos tipos de autenticación pero por facilidad y costos se ha escogido *PEAP-MSCHAPv2*.

PEAP-MSCHAPv2 ofrece un esquema de seguridad robusto y suficiente para una empresa, mediante nombres de usuario y contraseñas autentica usuarios; adicionalmente el servidor tiene instalado un certificado digital para su autenticación, este esquema autentica a los dos participantes.

Toda la información del cliente inalámbrico hasta el servidor (en el caso de la autenticación) o del cliente inalámbrico a los servidores, dependiendo del flujo de información es encriptado con *AES* que es muy robusto y difícil de romper.

3.7 ADMINISTRACIÓN DE RED

El *software* para administración de red deberá ser compatible con el estándar más usado, para este propósito es *SNMP*, con esto se asegura la compatibilidad con dispositivos de diferentes marcas que soporten el estándar.

La mayoría de equipos de conectividad son compatibles con las versiones de *SNMP v1* y *v2c*, pero *SNMP* tiene una última versión que es la *v3* que tiene funcionalidades parecidas a los anteriores pero incorpora seguridades como: encriptación y autenticación, mediante el uso de contraseñas.

El sistema de administración de red debe tener las siguientes características:

- Administración de Redes Remotas
- Compatibilidad con *VLANs*
- Compatibilidad de equipos multimarca
- Compatibilidad con *SNMP v1*, *v2c* y *v3*
- Esquematizar la arquitectura de la red
- Administración remota de equipos
- Compatibilidad con ruteadores, *switches*, *access points*, etc.

Los equipos para el rediseño de la red se detallan en la Tabla 3 - 74

Cantidad	Equipo	Características
1	Switch Capa 3	48 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T y 2 puertos <i>stack</i>
7	Switch Capa 3	24 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T y 2 puertos <i>stack</i>
2	Switch Capa 3	24 puertos 10/100 Base T, 2 puertos 10/100/1000 Base T
4	Ruteador	1 puerto WAN V.35 y 1 puerto LAN 10/100 Base T
1	Ruteador	2 puertos WAN V.35 y 1 puerto LAN 10/100 Base T
1	Ruteador	4 puertos WAN V.35 y 1 puerto LAN 10/100 Base T
3	Sistema Unificado de Seguridad	Usuarios ilimitados
3	Sistema Unificado de Seguridad	Hasta 25 usuarios
6	Centrales Telefónicas IP	
13	Access Points	802.11g, 1 puerto LAN 10/100 Base T

Tabla 3-74: Equipos necesarios para la Reingeniería de la Red

En total son 41 equipos de conectividad que son los que se van a administrar y monitorear con el Sistema de Administración de Red; para adquirir un NMS se debe saber cuántos dispositivos se van a administrar, porque según el número de dispositivos se compra la licencias o las versiones del sistema.

Las marcas de los equipos predominantes en el Rediseño de la Red son 3COM y Cisco, por lo que se tienen dos alternativas para equipos y el Sistema de Administración de Red; en el Capítulo 4 se escogerá una de las alternativas según el Costo / Beneficio de la solución.

En este caso se tiene Sistemas de Administración de Red de los dos fabricantes que predominan los equipos de conectividad, Cisco y 3COM. Estos Sistemas de Administración de Red son compatibles con el protocolo SNMP que es abierto y compatible; si por algún motivo se desea incluir un equipo de otro fabricante, estos sistemas podrán administrarlo, no con tanta funcionalidad como si fueran de la misma marca pero lo podrán hacer.

En el caso de 3COM el Sistema de Administración de Red más apropiado es 3COM Network Director, que permite esquematizar la red, administración remota de los equipos de conectividad 3COM y de otras marcas, siempre y cuando sean compatibles con SNMP.

Adicionalmente este sistema incluye gratuitamente *3COM Network Access Manager*, como su nombre lo indica éste es un sistema para administración de usuarios, está totalmente integrado con *Microsoft Active Directory* y el Servicio *IAS* que trabaja como servidor *RADIUS* para la autenticación de usuarios en *Windows*.

Este sistema facilita totalmente la gestión de usuarios, maneja grupos de usuarios y sus permisos, tipos de autenticación, relaciona puertos del *switch* con determinados usuarios o permite un solo usuario por puerto, etc. *3COM Network Access Manager* y *3COM Network Director* están totalmente integrados brindando control y gestión total de la red.

Cisco tiene un Sistema de Administración de Red llamado *CiscoWorks*; existen algunas versiones éstas son:

- *CiscoWorks Small Network Management Solutions*
- *CiscoWorks LAN Management Solutions*

CiscoWorks Small Management Solutions es un *NMS* para empresas que tengan menos de 40 dispositivos como ruteadores, *switches*, *access points*, etc. En la Tabla 3 - 74, se tiene una lista de 41 equipos. Pero si se escoge la opción de *Cisco* las centrales telefónicas *IP* no son equipos físicos sino son versiones especiales de *Cisco IOS*, por lo que serian 35 dispositivos y están dentro de los dispositivos que puede soportar esta versión de *CiscoWorks*.

CiscoWorks Small Management Solutions incluye *What's Up Gold* para monitoreo de equipos de conectividad de otros vendedores así como servidores, impresoras, etc. Esto se logra por la compatibilidad con el protocolo *SNMP*.

Los componentes que tiene *CiscoWorks Small Management Solutions* son:

- Manejador de Recursos Básico, maneja inventario, configuración, y actualizaciones de software de ruteadores y *switches Cisco*.
- *CiscoView* provee una base de datos común para que una aplicación muestre el esquema de red, sea ésta *Cisco* o no.
- Servicios Comunes, es la base de *CiscoWorks* que da el modelo de almacenamiento de datos, usuarios, privilegios de acceso y protocolos de seguridad.

CiscoWorks LAN Management Solutions es un NMS para gran cantidad de usuarios desde 100 hasta 5000. Cada usuario es un equipo de conectividad no un computador. *CiscoWorks LAN Management Solutions* ya no necesita de *What's Up Gold* para mostrar el mapa de la red ni su arquitectura, éste tiene un módulo propio de *Cisco* para realizar esta tarea.

Las versiones de menos dispositivos son:

- *CiscoWorks LAN Management Solutions* para 1 servidor y 100 dispositivos
- *CiscoWorks LAN Management Solutions* para 1 servidor y 300 dispositivos

CiscoWorks LAN Management Solutions tiene una administración más avanzada de los equipos de red, pero también su costo es casi el doble que la solución para pequeñas y medianas empresas. La mínima cantidad de dispositivos que viene incluido en el precio de la licencia es 100. Esta cantidad de dispositivos está presente en grandes empresas de más de 500 empleados aproximadamente.

CiscoWorks LAN Management Solutions tiene los siguientes módulos:

- Manejador de fallas en los dispositivos, provee detección detallada en tiempo real, análisis y reportes de las fallas de los dispositivos.

- Manejador de Campo, configura, administra y visualiza complejas infraestructuras capa 2, incluyendo *VLANs* y manejo de redes *ATM*, análisis de rutas, usuarios y mapeo de topología.
- Manejador de Recursos Básico, maneja inventario, configuración, y actualizaciones de *software* de ruteadores y *switches Cisco*.
- Monitor de rendimiento de la red, ofrece mediciones proactivas del tiempo de respuesta de la red y la disponibilidad en tiempo real, adicionalmente realiza un análisis del histórico de problemas de congestión y latencia.
- *CiscoView*, es un panel gráfico de *Cisco* que permite una interacción simple del usuario con los dispositivos para cambiar su configuración y monitorearlos.
- Servicios Comunes, es la base de *CiscoWorks* que da el modelo de almacenamiento de datos, usuarios, privilegios de acceso y protocolos de seguridad.

CAPÍTULO 4
ANÁLISIS DE COSTOS DE LA
SOLUCIÓN

4 ANÁLISIS DE COSTOS DE LA SOLUCIÓN

4.1 COSTOS DE LAS SOLUCIONES

4.1.1 EQUIPOS 3COM⁴³

4.1.1.1 Equipos de Conectividad

4.1.1.1.1 Switches

Switch 3COM 5500 EI 52 puertos

- **Puertos:** 48 puertos 10 *Base-T* / 100 *Base-TX*, 4 puertos *Gigabit SFP*, puerto de alimentación *RPS* (-48 *VDC*).
- **Rendimiento:** Capacidad de transmisión de 12,8 *Gbps*, 9,5 millones de paquetes por segundo, 16.000 direcciones *MAC*, máximo.
- **Stack:** capacidad de *stack* hasta 8 unidades, *stack* mediante 3COM *XRN* en configuración maestro / esclavo con puertos *SFP*.
- **Protocolos Capa 2:** *IEEE 802.Q VLANs*, *LACP 802.3ad*, control de flujo *802.3x full-duplex*, *STP 802.1D*, *RSTP 802.1w*, Arranque rápido con protección *BDPU*, filtrado *multicast IGMP v1/v2*
- **Protocolos Capa 3:** Ruteo basado en *hardware*, *ECMP*, *ARP*, interfaces virtuales, ruteo estático / dinámico, *RIP v1 / v2*, *OSPF*, transmisión de Capa 3 *ASIC*, *PIM-DM*, *PIM-SM*, *snooping IGMP v1/v2*, *Relay DHCP*.
- **Resistencia contra fallos:** *LACP IEEE 802.3ad*, unidades de *switch hot-swappable*, el *RPS DC* proporciona redundancia de alimentación

⁴³ Características obtenidas de www.3com.com y precios de www.insight.com

N+1, cambio sin discontinuidades entre modos *AC* y *DC* en caso de fallo.

- **Convergencia:** *Round robin* ponderada (*WRR*), asignación de colas equitativa ponderada (*WFF*) / por estricta prioridad (*SPQ*), Clase de Servicio / Calidad de Servicio *IEEE 802.1p*, clasificación, priorización y filtrado *IPv6*, limitación de velocidad de entrada y salida, administración de la capacidad de transmisión basada en *web* caché.
- **Seguridad:** *RADIUS*; autenticación *PAP/CHAP/EAPoL* (*EAP* sobre *LAN*); contabilidad de sesión; *SSH v1.5*; listas de control de acceso (*ACLs*); filtrado de paquetes; encriptación *SNMP v3*; inicio de sesión de red *IEEE 802.1X*; autenticación, auto-iniciación de *VLAN* y perfiles de *QoS*; privilegios de acceso multinivel; recuperación de contraseña de administración; registros de actividad de administración.
- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI* *RMON-1*, *SMON*.
- **Número de Parte:** 3CR17162-91
- **Precio:** \$ 2700,00 + IVA



Figura 4-1: Switch 3COM 5500 EI 52 puertos

Switch 3COM 5500 EI 28 puertos

- **Puertos:** 24 puertos 10 *Base-T* / 100 *Base-TX*, 4 puertos *Gigabit SFP*, puerto de alimentación *RPS* (-48 *VDC*),
- **Rendimiento:** Capacidad de transmisión de 12,8 *Gbps*, 9,5 millones de paquetes por segundo, 16.000 direcciones *MAC*, máximo.
- **Stack:** capacidad de *stack* hasta 8 unidades, *stack* mediante 3COM *XRN* en configuración maestro / esclavo con puertos *SFP*.
- **Protocolos Capa 2:** *IEEE 802.Q VLANs*, *LACP 802.3ad*, control de flujo *802.3x full-duplex*, *STP 802.1D*, *RSTP 802.1w*, Arranque rápido con protección *BDPU*, filtrado *multicast IGMP v1/v2*

- **Protocolos Capa 3:** Ruteo basado en *hardware*, *ECMP*, *ARP*, interfaces virtuales, ruteo estático / dinámico, *RIP v1 / v2*, *OSPF*, transmisión de Capa 3 *ASIC*, *PIM-DM*, *PIM-SM*, *snooping IGMP v1 / v2*, *Relay DHCP*.
- **Resistencia contra fallos:** *LACP IEEE 802.3ad*, unidades de *switch hot-swappable*, *RPS DC* proporciona redundancia de alimentación N+1, cambio sin discontinuidades entre modos *AC* y *DC* en caso de fallo.
- **Convergencia:** *Round Robin* ponderada (*WRR*), asignación de colas equitativa ponderada (*WFF*) / por estricta prioridad (*SPQ*), Clase de Servicio / Calidad de Servicio *IEEE 802.1p*, clasificación, priorización y filtrado *IPv6*, limitación de velocidad de entrada y salida, administración de capacidad de transmisión basada en *web* caché.
- **Seguridad:** *RADIUS*; autenticación *PAP/CHAP/EAPoL* (*EAP* sobre *LAN*); contabilidad de sesión; *SSH v1.5*; listas de control de acceso (*ACLs*); filtrado de paquetes; encriptación *SNMP v3*; inicio de sesión de red *IEEE 802.1X*; autenticación, auto-iniciación de *VLAN* y perfiles de *QoS*; privilegios de acceso multinivel; recuperación de contraseña de administración; registros de actividad de administración.
- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI* *RMON-1*, *SMON*
- **Número de Parte:** 3CR17161-91
- **Precio:** \$ 1200 + IVA



Figura 4-2: Switch 3COM 5500 EI 28 puertos

Switch 3COM 4500 EI 26 puertos

- **Puertos:** 24 puertos 10 *BASE-T* / 100 *BASE-TX* con auto-negociación configurados como auto *MDI / MDIX*; 2 pares de puertos *Gigabit* de uso dual: configurables por el usuario para *RJ45* (cobre), o interfaces basadas en *SFP* (fibra).

- **Rendimiento:** Capacidad de transmisión hasta 8,8 *Gbps*, hasta 6,5 millones de paquetes por segundo, y 8.000 direcciones *MAC*.
- **Stack:** Hasta ocho *switches*, o 384 puertos 10/100; Dirección *IP* única e interfaces de administración para control del *stack*.
- **Protocolos Capa 2:** *VLANs* basadas en puerto (802.1Q): 256, 802.3ad (*LACP*), agregación manual, grupos de troncal: 13 grupos (26 puertos), 8 puertos 10/100 ó 2 puertos *Gigabit* por grupo, auto-negociación de velocidad de puerto y dúplex, control de flujo *full-duplex* 802.3x, control de flujo de la presión trasera para el modo *half-duplex*, 802.1D (*STP*), 802.1w (*RSTP*), protección *BPDU* incluida en Arranque Rápido, *snooping IGMP* (Protocolo de gestión de grupos de Internet) v1 y v2, Analizador *IGMP*, filtrado para 128 grupos *multicast*
- **Protocolos Capa 3:** Ruteo basado en *hardware*, rutas estáticas: 12 además de la dirección por defecto, entradas *ARP* dinámicas / estáticas: 1990 / 10, interfaces *IP*: 4, *RIP*, v1 y v2: 2.000 rutas por defecto y 10 rutas mediante aprendizaje local, *snooping IGMP* v1 y v2, *Relay DHCP*: 2 KB máx.
- **Convergencia:** Ocho colas *hardware* por puerto, *CoS / QoS* 802.1p en salida, *DSCP EF* para priorización de tráfico *VoIP*, *round robin* ponderada (*WRR*), limitación de velocidad de salida, basada en puerto, bloqueo de aplicaciones y protocolos.
- **Seguridad:** Autenticación de usuario 802.1X: autenticación *RADIUS*, múltiples usuarios por puerto mediante fijación a la dirección *MAC*, asignación automática de puerto de *VLANs*, múltiples definiciones de dominio de servidor *RADIUS*, *RADA*; administración segura mediante *SSH v2* o *SNMPv3*, registros de actividad de administración automáticamente grabados para su análisis detallado, recuperación de contraseña de administración.
- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI* *RMON-1*, *SMON*
- **Número de Parte:** 3CR17561-91
- **Precio:** \$ 500 + IVA



Figura 4-3: Switch 3COM 4500 EI 26 puertos

Switch 3COM 5500 EI PWR 52 puertos

- **Puertos:** 48 puertos 10 *Base-T* / 100 *Base-TX*, 4 puertos *Gigabit SFP*, puerto de alimentación *RPS* (-48 *VDC*).
- **Rendimiento:** Capacidad de transmisión de 12,8 *Gbps*, 9,5 millones de paquetes por segundo, 16.000 direcciones *MAC*, máximo.
- **Stack:** capacidad de *stack* hasta 8 unidades, *stack* mediante 3COM *XRN* en configuración maestro / esclavo con puertos *SFP*.
- **Protocolos Capa 2:** *IEEE 802.Q VLANs*, *LACP 802.3ad*, control de flujo *802.3x full-duplex*, *STP 802.1D*, *RSTP 802.1w*, Arranque rápido con protección *BDPU*, filtrado *multicast IGMP v1/v2*
- **Protocolos Capa 3:** Ruteo basado en *hardware*, *ECMP*, *ARP*, interfaces virtuales, ruteo estático / dinámico, *RIP v1 / v2*, *OSPF*, transmisión de Capa 3 *ASIC*, *PIM-DM*, *PIM-SM*, *snooping IGMP v1/v2*, *Relay DHCP*.
- **Resistencia contra fallos:** *LACP IEEE 802.3ad*, unidades de *switch hot-swappable*, el *RPS DC* proporciona redundancia de alimentación N+1, cambio sin discontinuidades entre modos *AC* y *DC* en caso de fallo.
- **Convergencia:** *Round robin* ponderada (*WRR*), asignación de colas equitativa ponderada (*WFF*) / por estricta prioridad (*SPQ*), Clase de Servicio / Calidad de Servicio *IEEE 802.1p*, clasificación, priorización y filtrado *IPv6*, limitación de velocidad de entrada y salida, administración de la capacidad de transmisión basada en *web cache*.
- **Seguridad:** *RADIUS*; autenticación *PAP/CHAP/EAPoL* (*EAP* sobre *LAN*); contabilidad de sesión; *SSH v1.5*; listas de control de acceso (*ACLs*); filtrado de paquetes; encriptación *SNMP v3*; inicio de sesión de red *IEEE 802.1X*; autenticación, auto-iniciación de *VLAN* y perfiles

de QoS; privilegios de acceso multinivel; recuperación de contraseña de administración; registros de actividad de administración.

- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI* *RMON-1*, *SMON*.
- **PoE:** *IEEE 802.3af*
- **Número de Parte:** 3CR17172-91
- **Precio:** \$ 3450,00 + IVA



Figura 4-4: *Switch 3COM 5500 EI PWR 52 puertos*

Switch 3COM 5500 EI PWR 28 puertos

- **Puertos:** 24 puertos 10 *Base-T* / 100 *Base-TX*, 4 puertos *Gigabit SFP*, puerto de alimentación *RPS (-48 VDC)*,
- **Rendimiento:** Capacidad de transmisión de 12,8 *Gbps*, 9,5 millones de paquetes por segundo, 16.000 direcciones *MAC*, máximo.
- **Stack:** capacidad de *stack* hasta 8 unidades, *stack* mediante 3COM *XRN* en configuración maestro / esclavo con puertos *SFP*.
- **Protocolos Capa 2:** *IEEE 802.Q VLANs*, *LACP 802.3ad*, control de flujo *802.3x full-duplex*, *STP 802.1D*, *RSTP 802.1w*, Arranque rápido con protección *BDPU*, filtrado *multicast IGMP v1/v2*
- **Protocolos Capa 3:** Ruteo basado en *hardware*, *ECMP*, *ARP*, interfaces virtuales, ruteo estático / dinámico, *RIP v1 / v2*, *OSPF*, transmisión de Capa 3 *ASIC*, *PIM-DM*, *PIM-SM*, *snooping IGMP v1 / v2*, *Relay DHCP*.
- **Resistencia contra fallos:** *LACP IEEE 802.3ad*, unidades de *switch hot-swappable*, *RPS DC* proporciona redundancia de alimentación *N+1*, cambio sin discontinuidades entre modos *AC* y *DC* en caso de fallo.
- **Convergencia:** *Round Robin ponderada (WRR)*, asignación de colas equitativa ponderada (*WFF*) / por estricta prioridad (*SPQ*), Clase de

Servicio / Calidad de Servicio *IEEE 802.1p*, clasificación, priorización y filtrado *IPv6*, limitación de velocidad de entrada y salida, administración de capacidad de transmisión basada en *web cache*.

- **Seguridad:** *RADIUS*; autenticación *PAP/CHAP/EAPoL* (*EAP* sobre *LAN*); contabilidad de sesión; *SSH v1.5*; listas de control de acceso (*ACLs*); filtrado de paquetes; encriptación *SNMP v3*; inicio de sesión de red *IEEE 802.1X*; autenticación, auto-iniciación de *VLAN* y perfiles de *QoS*; privilegios de acceso multinivel; recuperación de contraseña de administración; registros de actividad de administración.
- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI* *RMON-1*, *SMON*
- **PoE:** *IEEE 802.3af*
- **Número de Parte:** 3CR17171-91
- **Precio:** \$ 2050 + IVA



Figura 4-5: Switch 3COM 5500 EI PWR 28 puertos

Switch 3COM 4500 EI PWR 26 puertos

- **Puertos:** 24 puertos 10 *BASE-T* / 100 *BASE-TX* con auto-negociación configurados como auto *MDI / MDIX*; 2 pares de puertos *Gigabit* de uso dual: configurables por el usuario para *RJ45* (cobre), o interfaces basadas en *SFP* (fibra).
- **Rendimiento:** Capacidad de transmisión hasta 8,8 *Gbps*, hasta 6,5 millones de paquetes por segundo, y 8.000 direcciones *MAC*.
- **Stack:** Hasta ocho *switches*, o 384 puertos 10/100; Dirección *IP* única e interfaces de administración para control del *stack*.
- **Protocolos Capa 2:** *VLANs* basadas en puerto (*802.1Q*): 256, *802.3ad* (*LACP*), agregación manual, grupos de troncal: 13 grupos (26 puertos), 8 puertos 10/100 ó 2 puertos *Gigabit* por grupo, auto-negociación de velocidad de puerto y dúplex, control de flujo *full-*

duplex 802.3x, control de flujo de la presión trasera para el modo *half-duplex*, *802.1D (STP)*, *802.1w (RSTP)*, protección *BPDU* incluida en Arranque Rápido, *snooping IGMP* (Protocolo de gestión de grupos de Internet) v1 y v2, Analizador *IGMP*, filtrado para 128 grupos *multicast*

- **Protocolos Capa 3:** Ruteo basado en *hardware*, rutas estáticas: 12 además de la dirección por defecto, entradas *ARP* dinámicas / estáticas: 1990 / 10, interfaces *IP*: 4, *RIP v1 / v2*: 2.000 rutas por defecto y 10 rutas mediante aprendizaje local, *snooping IGMP v1 y v2*, *Relay DHCP*: 2 KB máx.
- **Convergencia:** Ocho colas *hardware* por puerto, *CoS / QoS 802.1p* en salida, *DSCP EF* para priorización de tráfico *VoIP*, *round robin ponderada (WRR)*, limitación de velocidad de salida, basada en puerto, bloqueo de aplicaciones y protocolos.
- **Seguridad:** Autenticación de usuario *802.1X*: autenticación *RADIUS*, múltiples usuarios por puerto mediante fijación a la dirección *MAC*, asignación automática de puerto de *VLANs*, múltiples definiciones de dominio de servidor *RADIUS*, *RADA*; administración segura mediante *SSH v2* o *SNMP v3*, registros de actividad de administración automáticamente grabados para su análisis detallado, recuperación de contraseña de administración.
- **Tipos de Administración:** *GUI* basada en *web*, *SNMP*, *Telnet*, *CLI*, *RMON-1*, *SMON*
- **PoE:** *IEEE 802.3af*
- **Número de Parte:** 3CR17571-91
- **Precio:** \$ 1220 + IVA



Figura 4-6: Switch 3COM 4500 EI PWR 26 puertos

4.1.1.1.2 Transceiver Switches

Transceiver 3COM 1000 Base-T SFP.

- **Número de Parte:** 3CSFP93
- **Precio:** \$ 150,00 + IVA



Figura 4-7: Transceiver 3COM 1000 Base T SFP

4.1.1.1.3 Ruteadores

Ruteador 3COM 5012

- **Puertos:** Un 10/100 Base-T, un serial de alta velocidad sincrónico y asincrónico, uno de consola, un auxiliar; una ranura *MIM* y dos *SIC*.
- **Interfaces WAN:** *RDSI*, *ADSL*, *E1*, *T1*, serial de alta velocidad, *X.25*, *PPP*, *PPPoE*, *MP*, *Frame Relay*, *HDLC / SDLC*.
- **Interfaces LAN:** *Ethernet 10/100*, *10/100/1000*
- **Ruteo WAN:** *IP*, *IPX*, *OSPF*, *BGP-4*, *IS-IS* Integrado, *RIP v1 / v2*, ruteo estático, *VPN MPLS L2 y L3*
- **Seguridad:** *Stateful Firewall*, *VPN (L2TP, GRE, IPSec)*, *ACLs*, *NAT*, *RADIUS*, *PAP/CHAP*, *TACACS+*, certificados *X.509*
- **Convergencia:** *QoS*, *Multicast IGMP*, *PIM-SM*, *PIM-DM*, *VLAN IEEE 802.1q*, ruteo *Inter-VLAN*, *Multi-links*
- **Resistencia ante fallos:** *VRRP*, Centro de *Backup* (configuración / Puerto), Centro de Control de Marcación, *multilink*, soporte de imágenes duales.
- **SDRAM:** 128 MB
- **Flash:** 32 MB
- **Número de Parte:** 3C13701

- **Precio:** \$ 800 + IVA



Figura 4-8: Ruteador 3COM 5012

4.1.1.1.4 Tarjetas para Ruteadores

Tarjeta Ruteador SIC 3COM un Puerto Serial

- **Puertos:** 1
- **Conector:** 1 DB28
- **Interfaz de servicio:** serial sincrónico o asincrónico
- **Interfaz Estándar:** V.24, V.35, X.21, RS-232, DCE, DTE
- **Máxima velocidad:**
 - V.24: 64 Kbps sincrónico
 - V.35: 2.048 Mbps sincrónico
 - X.21: 2.048 Mbps sincrónico
 - RS-232: 115.2 Kbps asincrónico
- **Número de Parte:** 3C13715
- **Precio:** \$ 170,00 + IVA



Figura 4-9: Tarjeta 3COM 1 puerto serial

Tarjeta Ruteador SIC 3COM con dos Puertos Seriales

- **Puertos:** 2
- **Conector:** 2 DB28
- **Interfaz de servicio:** serial sincrónico o asincrónico

- **Interfaz Estándar:** V.24, V.35, X.21, RS-232, DCE, DTE
- **Máxima velocidad:**
 - **V.24:** 64 Kbps sincrónico
 - **V.35:** 2.048 Mbps sincrónico
 - **X.21:** 2.048 Mbps sincrónico
 - **RS-232:** 115.2 Kbps asincrónico
- **Número de Parte:** 3C13762
- **Precio:** \$ 400,00 + IVA



Figura 4-10: Tarjeta 3COM 2 puertos seriales

Tarjeta Ruteador 3COM MIM 4 Puertos Seriales

- **Puertos:** 4 puertos seriales sincrónicos / asincrónicos
- **Conector:** DB-28
- **Velocidad Máxima:**
 - **V.24:** 64 Kbps sincrónico
 - **V.35:** 2.048 Mbps sincrónico
 - **X.21:** 2.048 Mbps sincrónico
 - **RS-232:** 115.2 Kbps asincrónico
- **Número de Parte:** 3C13764
- **Precio:** \$ 800,00 + IVA



Figura 4-11: Tarjeta 3COM 4 puertos seriales

4.1.1.1.5 Cables para Ruteadores

Cable 3COM V.35 DCE

- **Conectores:** DB-28 macho a V.35 hembra
- **Longitud:** 3 m
- **Tipo de Cable de Red:** cable V.35
- **Tipo de Equipo Soportado:** DCE
- **Número de parte:** 3C13686
- **Precio:** \$ 80 + IVA

Cable 3COM V.35 DTE

- **Conectores:** DB-28 macho a V.35 macho
- **Longitud:** 3 m
- **Tipo de Cable de Red:** cable V.35
- **Tipo de Equipo Soportado:** DTE
- **Número de parte:** 3C13685
- **Precio:** \$ 80 + IVA

4.1.1.1.6 Access Points

Access Point 3COM 7760 802.11 a/b/g PoE

- **Usuarios soportados:** hasta 64 usuarios simultáneos.
- **Estándares compatibles:** 802.11a, 802.11b, 802.11g, 802.11i, 802.3, 802.3af, 802.1X, WEP, AES, WPA, WPA2, Certificado Wi-Fi.
- **Rango de operación:** 802.11a hasta 50 m y 802.11b/g hasta 100 m.
- **Antenas:** Dos externas de banda dual 2.4 / 5.15 GHz R-SMA
- **Seguridad:** WPA/WPA2 con encriptación AES y TKIP; 802.1X con EAP-TLS, EAP-TTLS y PEAP; WPA/WPA2 con autenticación PSK; direcciones MAC para autenticación y filtro; 802.1Q VLAN; múltiple SSID; cliente RADIUS AAA.

- **Administración:** soporta *SNMP v1/v2c*, administración remota mediante navegador *web* y línea de comandos por medio de *Telnet*.
- **Desempeño:** 108 *Mbps* Modo Super G
- **Consumo PoE:** 6 *W* máximo.
- **Número de Parte:** 3CRWE776075
- **Precio:** \$ 215,00 + IVA



Figura 4-12: Access Point 3COM 7760 802.11 a/b/g PoE

4.1.1.1.7 Sistema Unificado de Seguridad

Sistema Unificado de Seguridad 3COM X5

- **Puertos:** 6 puertos 10 *Base-T* / 100 *Base-TX* con auto-negociación, configurados como auto *MDI* / *MDIX*; 1 puerto serie (*RJ-45*)
- **Método de prevención de intrusiones:** Motor de supresión de amenazas de *TippingPoint*
- **Rendimiento de IPS :** 18 *Mbps*
- **Sesiones concurrentes de IPS:** 60.000
- **Filtros de ataques:** más de 2.300 filtros de ataques que proporcionan protección frente a *spyware*, gusanos, virus, troyanos, *phishing*, amenazas de *VoIP*, *DoS*, *P2P*, *IM*.
- **Actualizaciones de filtros de ataques:** se distribuyen automáticamente a todos los clientes con servicio de suscripción para dispositivos 3Com X5, mediante el Servicio de Actualización de Filtros de Ataques de Vacuna Digital.

- **Cuarentena:** aísla los dispositivos infectados de la red sin precisar de ningún *PC* cargado con *software* específico.
- **Rendimiento del *firewall*:** 50 *Mbps*
- **Políticas de *firewall*:** 100
- **Zonas de seguridad de *firewall*:** 16
- **Rendimiento de *VPN* (DES de 169 bits):** 40 *Mbps*
- **Sesiones concurrentes de cliente *VPN*:** 128
- **Encriptación *VPN*:** DES, 3DES, AES128, AES-192, AES-256
- **Soporte de cliente *VPN*:** IPsec nativo, L2TP/IPsec, PPTP/MPPE
- **Filtrado de contenidos *web*:** más de 15 millones de *URLs* filtradas; 40 categorías; listas negras/blancas de *URLs* personalizadas; servicio de suscripción a *SurfControl* integrado.
- **Modelado de tráfico:** Limitación de velocidad del tráfico entrante y saliente; modelado basado en políticas; el modelado de tráfico puede realizarse dentro de túneles *VPN*. Administración de ancho de banda
- **Seguridad:** Autenticación de servidor *RADIUS* y de base de datos local; *SNMP v1*, 2 y 3.
- **Administración:** Interfaz *web* mediante *HTTPS*; interfaz de línea de comandos mediante consola, *telnet*, *SSH*; soporte de Sistema de Administración de Seguridad (*SMS*) de *TippingPoint*.
- **Sistema Unificado de Seguridad 3COM X5 (25 usuarios) N/P:** 3CRTPX5-25-96; **Precio:** \$ 870,00 + IVA
- **Sistema Unificado de Seguridad 3COM X5 (usuarios ilimitados) N/P:** 3CRTPX5-U-96; **Precio:** \$ 1050,00 + IVA



Figura 4-13: Sistema Unificado de Seguridad 3COM X5

Vacuna Digital 3COM X5 Servicio de Actualización Filtros de Ataques *GOLD*. Incluye filtros de ataques actualizados, filtro de contenido *web*, soporte técnico telefónico, sustitución avanzada de *hardware*, y actualizaciones de *software*.

- **Número de parte:** 3CTPX5-DVGOLD
- **Precio:** \$ 560,00 + IVA

Vacuna Digital 3COM X5 Servicio de Actualización de Filtros de Ataques. Incluye filtros de ataques actualizados, soporte técnico telefónico, sustitución avanzada de *hardware*, y actualizaciones de *software*.

- **Número de parte:** 3CTPX5-DV
- **Precio:** \$ 400,00 + IVA

4.1.1.2 Centrales Telefónicas

Central Telefónica 3COM Asterisk

- **Capacidad de Usuarios:** Hasta 25 llamadas simultáneas y 50 usuarios.
- **Aplicaciones:** Atención automática, correo de voz, distribución automática de llamadas, respuesta de voz interactiva y conferencia.
- **Licencias:** no son requeridas licencias para activar teléfonos o conexiones con la *PSTN* al sistema.
- **FXO, FXS y Gateways T1 / E1:** el equipo integra 4 puertos análogos *FXO* y 4 *FXS*, además 4 puertos *LAN* para teléfonos *IP*. Si se requieren puertos *E1 / T1* o mas puertos análogos se puede adicionar uno o más *Gateway 3COM VCX* con los puertos necesarios.
- **Conexiones de Red:** 1 puerto *WAN Ethernet 10/100 Base T*.
- **Número de Parte:** 3CR10551A
- **Precio:** \$ 1580 + IVA



Figura 4-14: Central Telefónica 3COM Asterisk

4.1.1.3 Gateways IP

Gateway 3COM VCX 7111 8 puertos FXO

- **Soporte:** SIP
- **Puertos:**
 - 8 puertos analógicos FXO (RJ11)
 - 1 puerto LAN 10/100 Base T (RJ45)
 - 1 puerto serial para Administración (Consola)
- **Codecs de Voz:** G.711, G.723.1, G.729a, G.726
- **Número de Parte:** 3CRVG71114-07
- **Precio:** \$ 850 + IVA



Figura 4-15: Gateway 3COM VCX 7111 8 puertos FXO

Gateway 3COM VCX 7111 4 puertos FXO

- **Soporte:** SIP
- **Puertos:**
 - 4 puertos analógicos FXO (RJ11)
 - 1 puerto LAN 10/100 Base T (RJ45)
 - 1 puerto serial para Administración (Consola)

- **Codecs de Voz:** G.711, G.723.1, G.729a, G.726
- **Número de Parte:** 3CRVG71113-07
- **Precio:** \$ 680,00 + IVA



Figura 4-16 Gateway 3COM VCX 7111 4 puertos FXO

4.1.1.4 Teléfonos IP

Teléfono IP 3COM 3101 Teléfono Básico

- **Control de llamadas:** soporta plataformas 3Com NBX y VCX SIP
- **Soporte:** PoE, DHCP
- **Puertos:** 2 puertos Ethernet 10/100 Base TX
- **Calidad de Servicio:** 802.1p, 802.1Q (VLAN), 802.3, ToS
- **Codecs de Voz:** ADPCM, G.711, G.729ab
- **Jitter Buffer:** Adaptivo
- **Pantalla:** 160 x 33 pixeles
- **Tamaño de Trama RTP:** 20/30 ms.
- **Supresión de silencios:** soportada con G.729b
- **Número de Parte:** 3C10401B
- **Precio:** \$ 140,00 + IVA



Figura 4-17: Teléfono Básico 3COM 3101

Teléfono IP 3COM 3101 Teléfono Básico con Parlante

- **Control de llamadas:** soporta plataformas 3Com NBX y VCX SIP
- **Soporte:** PoE, DHCP
- **Puertos:** 2 puertos Ethernet 10/100 Base TX
- **Calidad de Servicio:** 802.1p, 802.1Q (VLAN), 802.3, ToS
- **Codecs de Voz:** ADPCM, G.711, G.729ab
- **Jitter Buffer:** Adaptivo
- **Pantalla:** 160 x 33 pixeles
- **Tamaño de Trama RTP:** 20/30 ms.
- **Supresión de silencios:** soportada con G.729b
- **Número de Parte:** 3C10401SPKRB
- **Precio:** \$ 160,00 + IVA



Figura 4-18: Teléfono Básico con Parlante 3COM 3101

Teléfono IP 3COM 3102 Teléfono de Negocios

- **Control de llamadas:** soporta plataformas 3COM NBX y VCX SIP
- **Soporte:** PoE, DHCP
- **Puertos:** 2 puertos Ethernet 10/100 Base TX
- **Headset jack:** conector tipo RJ-9
- **Calidad de Servicio:** 802.1p, 802.1Q (VLAN), 802.3, ToS
- **Codecs de Voz:** ADPCM, G.711, G.729ab
- **Jitter Buffer:** Adaptivo
- **Pantalla:** 160 x 33 pixeles
- **Tamaño de Trama RTP:** 20 / 30 ms.
- **Supresión de silencios:** soportada con G.729b
- **Número de Parte:** 3C10402B
- **Precio:** \$ 210,00 + IVA



Figura 4-19: Teléfono de Negocios 3COM 3102

4.1.1.5 Software de Administración de Red

3COM Network Director

- Es un paquete autónomo que monitoriza y controla una red de datos y telefonía, incluyendo *switches*, *routers*, puntos de acceso inalámbrico, componentes de telefonía *IP*, estaciones terminales y servidores.
- Las capacidades avanzadas de recuperación de configuraciones y actualización de agentes *software* para productos 3COM de *LAN* y *WAN*, simplifican la administración de red pudiendo mejorar su rendimiento y fiabilidad.
- El completo registro de eventos proporciona descripciones claras y la gravedad de los problemas de red.
- La potente monitorización de rendimiento detecta los cuellos de botella y otros problemas de la red; los datos históricos indican tendencias para facilitar predicciones del rendimiento futuro de la red.
- Los indicadores de resolución avanzada de problemas presentan los datos de *RMON* estándar en *switches*
- La recuperación, el mapeo de red automáticos y precisos, incluyendo vistas detalladas a niveles de Capa 2 y Capa 3 con actualizaciones de estado en tiempo real, muestran todos los equipos de red de datos, voz e inalámbrico; todos los enlaces de conexión, las estaciones terminales y los servidores; las trazas de rutas de datos entre entidades de red y las asociaciones *VLAN* de puertos y dispositivos
- La administración de elementos gráficos simplifica la administración de los *switches* (*Switch Manager*) y los *ruteadores* (*Router Manager*)
- **Número de Parte:** 3C15500
- **Precio:** \$ 2325,00 + IVA

3COM Network Access Manager se incluye gratis con *3COM Network Director*, a continuación se detallan sus características.

3COM Network Access Manager

- Maneja las Políticas de Control de Acceso a la Red, incrementa capacidades avanzadas de seguridad para *switches* y *access points* inalámbricos controlando el acceso a la red de usuarios y computadores.
- *3COM Network Access Manager* está totalmente integrado con *Active Directory* para el manejo de usuarios en un dominio corporativo. Incrementa la seguridad de la red al integrarse también con *IAS (Internet Authentication Service)*, que va a ser utilizado como servidor *RADIUS* para la autenticación de usuarios de la red.
- Simplifica la Administración de Acceso a la Red, simplifica la seguridad perimetral mediante el fácil control de acceso a la red con *Microsoft Active Directory*.
- Las reglas de control de accesos no solo deciden si un usuario o un computador pueden entrar a la red, sino que asignan la *VLAN* correspondiente y los parámetros de *QoS* según su perfil.
- Permite al administrador asignar privilegios de acceso a usuarios o computadores, o a un grupo de *Active Directory*.

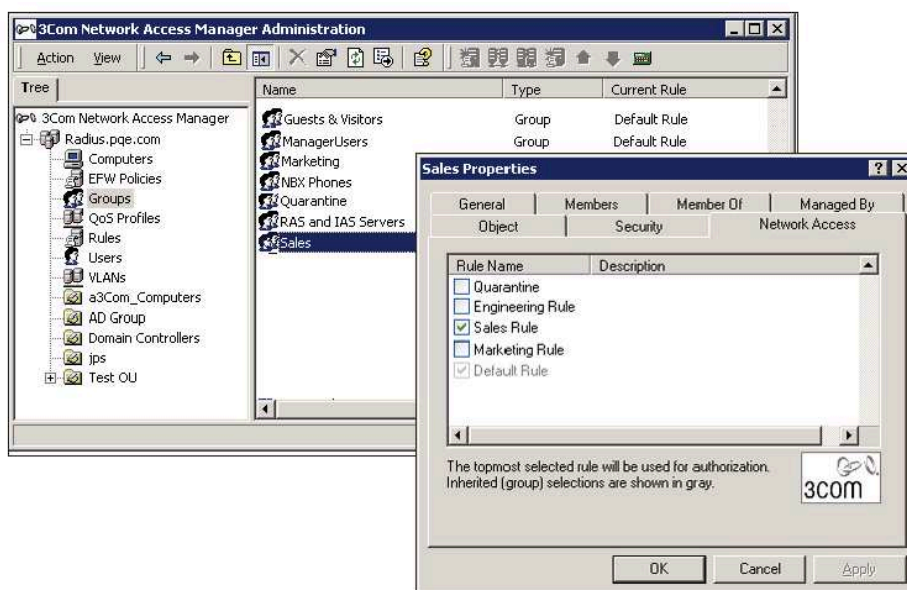


Figura 4-20: 3COM Access Manager

4.1.2 EQUIPOS CISCO⁴⁴

4.1.2.1 Equipos de Conectividad

4.1.2.1.1 Switches

Switch Cisco 3750-24TS-S 24 puertos 10/100 Base T

- **Puertos:** 24 puertos 10/100 Base T, 1 puerto de administración RJ-45, 2 puertos *stack* RJ-45, 2 puertos SFP.
- **Memoria Flash:** 16 MB
- **Memoria RAM:** 128 MB
- **Métodos de Autenticación:** Kerberos, RADIUS, TACACS+, SSH.
- **Vida promedio del equipo:** 294.928 horas
- **Modo de comunicación:** Half-dúplex, full-dúplex
- **Protocolos:** Ruteo IP, soporta: DHCP, ARP, VLAN, IGMP snooping, IPv6, stackable, balanceo de carga, trunking.
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** SNMP v1/v2c/v3, RMON v1 / v2, Telnet.
- **Protocolos de Enrutamiento:** RIP v1 / v2, ruteo estático.
- **Estándares compatibles:** 802.3, 802.3u, 802.3z, 802.1D, 802.1Q, 802.3ab, 802.1p, 802.3ad (LACP), 802.1w, 802.1x, 802.1s.
- **Garantía:** Lifetime warranty.
- **Número de parte:** WS-C3750-24TS-S
- **Precio:** \$ 2900,00 + IVA



Figura 4-21: Switch Cisco 3750 24 puertos 10/100 Base T

⁴⁴ Características obtenidas de www.cisco.com y precios de www.insight.com

Switch Cisco 3750-24PS-S PoE 24 puertos 10/100 Base T

- **Puertos:** 24 puertos 10/100 Base T, 1 puerto de administración RJ-45, 2 puertos *stack* RJ-45, 2 puertos SFP.
- **Memoria Flash:** 16 MB
- **Memoria RAM:** 128 MB
- **Métodos de Autenticación:** Kerberos, RADIUS, TACACS+, Secure Shell (SSH)
- **Vida promedio del equipo:** 209.170 horas
- **Modo de comunicación:** Half-dúplex, full-dúplex
- **Protocolos:** Ruteo IP, soporta: DHCP, ARP, VLAN, IGMP snooping, IPv6, stackable, conector para fuente de poder redundante (RPS).
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** SNMP v1 / v2c / v3, RMON v1 / v2, Telnet.
- **PoE:** soportado
- **Protocolos de Enrutamiento:** RIP v1 / v2, HSPR, ruteo estático, IGMP v3.
- **Estándares compatibles:** 802.3u, 802.1D, 802.1Q, 802.1p, 802.3x, 802.3ad (LACP), 802.1w, 802.1x, 802.1s, 802.3af.
- **Garantía:** Lifetime Warranty.
- **Número de parte:** WS-C3750-24PS-S
- **Precio:** \$ 3500,00 + IVA



Figura 4-22: Switch Cisco 3750 24 puertos 10/100 Base T PoE

Switch Cisco 3750-48TS-S 48 puertos 10/100 Base T

- **Puertos:** 48 puertos 10/100 Base T, 1 puerto de administración RJ-45, 2 puertos *stack* RJ-45, 4 puertos SFP.
- **Memoria Flash:** 16 MB
- **Memoria RAM:** 128 MB

- **Métodos de Autenticación:** *RADIUS, TACACS+, SSH.*
- **Vida promedio del equipo:** 217.824 horas
- **Modo de comunicación:** *Half-dúplex, full-dúplex*
- **Protocolos:** Ruteo *IP*, soporta: *DHCP, ARP, VLAN, IGMP snooping, IP v6, stackable*, balaceo de carga.
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** *SNMP v1 / v2c / v3, RMON v1 / v2, Telnet.*
- **Protocolos de Enrutamiento:** *RIP v1 / v2*, ruteo estático *IP*.
- **Estándares compatibles:** *802.3, 802.3u, 802.3z, 802.1D, 802.1Q, 802.3ab, 802.1p, 802.3ad (LACP), 802.1w, 802.1x, 802.1s.*
- **Garantía:** *Lifetime warranty.*
- **Número de parte:** WS-C3750-48TS-S
- **Precio:** \$ 5050,00 + IVA



Figura 4-23: *Switch Cisco 3750 48 puertos 10/100 Base T*

Switch Cisco 3750-48PS-S PoE 48 puertos 10/100 Base T

- **Puertos:** 48 puertos 10/100 Base T, 1 puerto de administración RJ-45, 2 puertos *stack RJ-45*, 4 puertos *SFP*.
- **Memoria Flash:** 16 MB
- **Memoria RAM:** 128 MB
- **Métodos de Autenticación:** *Kerberos, RADIUS, TACACS+, SSH*
- **Vida promedio del equipo:** 166.408 horas
- **Modo de comunicación:** *Half-dúplex, full-dúplex*
- **Protocolos:** Ruteo *IP*, soporta: *DHCP, ARP, VLAN, IGMP snooping, IP v6, stackable*, conector para fuente de poder redundante (*RPS*).
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** *SNMP v1 / v2c / v3, RMON v1 / v2, Telnet.*

- **PoE:** soportado
- **Protocolos de Enrutamiento:** *RIP v1 / v2, HSPR, ruteo estático, IGMP v3.*
- **Estándares compatibles:** *802.3u, 802.1D, 802.1Q, 802.1p, 802.3x, 802.3ad (LACP), 802.1w, 802.1x, 802.1s, 802.3af.*
- **Garantía:** *Lifetime Warranty.*
- **Número de parte:** WS-C3750-48PS-S
- **Precio:** \$ 6150,00 + IVA



Figura 4-24: *Switch Cisco 3750 48 puertos 10/100 Base T PoE*

Switch Cisco 3650-24TS SMI 24 puertos

- **Puertos:** 24 puertos 10/100 Base T, 1 puerto de administración RJ-45, 1 puerto de consola RJ-45, 2 puertos SFP.
- **Memoria RAM:** 128 MB
- **Métodos de Autenticación:** *Kerberos, RADIUS, TACACS+, SSH2*
- **Vida promedio del equipo:** 326.100 horas
- **Modo de comunicación:** *Half-dúplex, full-dúplex*
- **Protocolos:** Ruteo IP, soporte: *DHCP, ARP, VLAN, IGMP snooping, IP v6.*
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** *SNMP v1 / v2c / v3, RMON v1 / v2, Telnet.*
- **Protocolos de Ruteo:** *OSPF, IGRP, BGP-4, RIP v1/v2, EIGRP, HSPR, DVMRP, PIM-SM, ruteo estático, PIM-DM, IGMP v3.*
- **Estándares compatibles:** *802.3, 802.3u, 802.3z, 802.1D, 802.1Q, 802.3ab, 802.1p, 802.3x, 802.3ad (LACP), 802.1w, 802.1x, 802.1s*
- **Garantía:** *Lifetime Warranty.*
- **Número de parte:** WS-C3650-24T-S
- **Precio:** \$ 2200,00 + IVA



Figura 4-25: *Switch Cisco 3560 24 puertos 100 Base T*

Switch Cisco 3650-24PT POE 24 puertos

- **Puertos:** 24 puertos 10/100 Base T, 1 puerto de administración RJ-45, 1 puerto de consola RJ-45, 2 puertos SFP.
- **Memoria RAM:** 128 MB
- **Métodos de Autenticación:** Kerberos, RADIUS, TACACS+, Secure Shell v.2 (SSH2)
- **Vida promedio del equipo:** 326.100 horas
- **Modo de comunicación:** Half-dúplex, full-dúplex
- **Protocolos:** Ruteo IP, soporte: DHCP, ARP, VLAN, IGMP snooping, IP v6.
- **Tamaño de la tabla de direcciones MAC:** 12 K entradas
- **Protocolos de Administración Remota:** SNMP v1 / v2c / v3, RMON v1 / v2, Telnet.
- **Power over Ethernet:** soportado
- **Protocolos de Ruteo:** OSPF, IGRP, BGP-4, RIP v1/v2, EIGRP, HSPR, DVMRP, PIM-SM, ruteo estático, PIM-DM, IGMP v3.
- **Estándares compatibles:** 802.3, 802.3u, 802.3z, 802.1D, 802.1Q, 802.3ab, 802.1p, 802.3x, 802.3ad (LACP), 802.1w, 802.1x, 802.1s, 802.3 af.
- **Garantía:** Lifetime Warranty.
- **Número de parte:** WS-C3560-24PS-SHCH
- **Precio:** \$ 2700,00 + IVA



Figura 4-26: *Switch Cisco 3560 24 puertos 100 Base T PoE*

4.1.2.1.2 Transceiver Switches

Módulo Transceiver Cisco SFP 1000 Base T

- **Slot Compatible:** 1 SFP
- **Interfaz:** 1 Ethernet 1000 Base T RJ45
- **Vida promedio del módulo:** 1 millón de horas
- **Estándares compatibles:** IEEE 802.3
- **Soporte:** Full-dúplex, reemplazo del módulo *hot swap*
- **Garantía:** 1 año.
- **Número de parte:** GLC-T
- **Precio:** \$ 300 + IVA



Figura 4-27: Módulo Transceiver SFP Cisco 1000 Base T

4.1.2.1.3 Cables para Stack

Cable Cisco StackWise 50 cm

- **Compatible:** Switches Cisco Catalyst serie 3750.
- **Longitud:** 50 cm.
- **Características:** Libre de Halógeno.
- **Garantía:** 1 año.
- **Número de parte:** CAB-STACK-50CM-NH
- **Precio:** \$ 122 + IVA.



Figura 4-28: Cable Cisco StackWise 50 cm

Cable Cisco StackWise 1 m

- **Compatible:** *Switches Cisco Catalyst serie 3750*
- **Tipo de cable de red:** cable para *stack*
- **Longitud:** 1 m
- **Características:** Libre de Halógeno
- **Garantía:** 1 año.
- **Número de parte:** CAB-STACK-1M-NH
- **Precio:** \$ 200 + IVA

4.1.2.1.4 Ruteadores

Ruteador Cisco 2801 Voice Bundle

- **Características Principales:** Protección *Firewall*, encriptación mediante *hardware*, soporte *MPLS*, filtro *URL*, soporte *VPN*.
- **Protocolo de Transporte de Red:** *IPSec*.
- **Protocolo de Administración Remota:** *SNMP v3*.
- **Algoritmos de encriptación:** *AES 128, 192 y 256 bits; DES, Triple DES*.
- **Interfaces:** 2 *Ethernet 10/100 Base T RJ45*, 1 *USB*, 1 de consola para administración *RJ45* y 1 auxiliar.
- **Slots de expansión:** 2 *HWIC*, 2 *AIM*, 1 *PVDM*, 1 *WIC*, 1 *VIC*, 1 *Compact Flash Card slot*
- **Características de Telefonía IP:** Cancelación de Eco (*G.168*)
- **Codecs de Voz:** *G.711, G.723.1, G.726, G.728, G.729*.
- **Memoria RAM:** instalada *256 MB* / soportada *384 MB*
- **Memoria Flash:** instalada *64 MB* / soportada *128 MB*
- **Sistema Operativo:** *Cisco IOS SP Service*
- **Software incluido:** *Cisco Call Manager Express* (licencia 24 teléfonos)
- **Garantía:** *Lifetime Warranty*.
- **Número de parte:** *CISCO2801-CCME/K9*

- **Precio:** \$ 2170,00 + IVA



Figura 4-29: Ruteador Cisco 2801 Voice Bundle

Ruteador Cisco 2811 Voice Bundle

- **Características Principales:** Diseño Modular, Protección *Firewall*, encriptación mediante *hardware*, soporte *MPLS*, filtro *URL*, soporte *VPN*.
- **Protocolo de Transporte de Red:** *IPSec*.
- **Protocolo de Administración Remota:** *SNMP v3*.
- **Algoritmos de encriptación:** *AES 128, 192 y 256 bits; DES, Triple DES*.
- **Interfaces:** 2 *Ethernet 10/100 Base T RJ45*, 2 *USB*, 1 de consola para administración *RJ45*, 1 auxiliar *RJ45*.
- **Método de autenticación:** *Secure Shell v2 (SSH2)*
- **Slots de expansión:** 4 *HWIC*, 2 *AIM*, 1 *PVDM*, 1 *NME*, 1 *Compact Flash Card slot*
- **Modem:** módulo voz / fax
- **Características de Telefonía IP:** Cancelación de Eco (*G.168*)
- **Codecs de Voz:** *G.711, G.723.1, G.726, G.728, G.729*.
- **Estándares compatibles:** *IEEE 802.3af*
- **Memoria RAM:** instalada 256 MB / soportada 768 MB
- **Memoria Flash:** instalada 64 MB / soportada 256 MB
- **Sistema Operativo:** *Cisco IOS SP Service*
- **Software incluido:** *Cisco Call Manager Express* (licencia 36 teléfonos)
- **Garantía:** *Lifetime Warranty*.
- **Número de parte:** *CISCO2811-CCME/K9*
- **Precio:** \$ 2360,00 + IVA



Figura 4-30: Ruteador Cisco 2811 Voice Bundle

Ruteador Cisco 2821 Voice Bundle

- **Características Principales:** Protección *Firewall*, soporte *MPLS*, filtro de contenido y *URL*.
- **Protocolo de Transporte de Red:** *IPSec*.
- **Protocolo de Administración Remota:** *RMON v2*, *Telnet*, *SNMP v3*.
- **Interfaces:** 2 *Ethernet 10/100 Base T RJ45*, 2 *USB*, 1 de consola para administración *RJ45*, 1 auxiliar *RJ45*.
- **Método de autenticación:** *Secure Shell v2 (SSH2)*
- **Slots de expansión:** 4 *HWIC*, 2 *AIM*, 3 *PVDM*, 1 *NME-X*, *EVM*.
- **Modem:** módulo voz / fax (32 puertos)
- **Características de Telefonía IP:** Cancelación de Eco (*G.168*)
- **Codecs de Voz:** *G.711*, *G.723.1*, *G.726*, *G.728*, *G.729*.
- **Estándares compatibles:** *IEEE 802.3af*
- **Memoria RAM:** instalada 256 MB / soportada 768 MB
- **Memoria Flash:** instalada 64 MB / soportada 256 MB
- **Sistema Operativo:** *Cisco IOS SP Service*
- **Software incluido:** *Cisco Call Manager Express* (licencia 48 teléfonos)
- **Garantía:** *Lifetime Warranty*.
- **Número de parte:** C2821-CCME/K9
- **Precio:** \$ 3440,00 + IVA



Figura 4-31: Ruteador Cisco 2821 Voice Bundle

4.1.2.1.5 Módulos Ruteadores

Módulo Cisco 1 puerto Serial Sincrónico / Asincrónico

- **Interfaz:** RS-232/449/530/V.35
- **Interfaz tipo:** 1 serial
- **Conector:** 60 pin D-Sub (DB-60)
- **Velocidad de transferencia:** 2.048 Mbps
- **Protocolo de Administración Remota:** SNMP
- **Garantía:** 1 año
- **Número de parte:** WIC-1T
- **Precio:** \$ 310,00 + IVA



Figura 4-32: Módulo Cisco 1 puerto Serial

Módulo Cisco 2 puerto Serial Sincrónico / Asincrónico

- **Interfaz:** RS-232/449/530/V.35
- **Interfaz tipo:** 2 serial
- **Velocidad de transferencia:** 2.048 Mbps
- **Protocolo de Administración Remota:** SNMP
- **Garantía:** 1 año
- **Número de parte:** WIC-2T
- **Precio:** \$ 530,00 + IVA



Figura 4-33: Módulo Cisco 2 puertos seriales

Módulo Cisco 4 puerto Serial Sincrónico / Asincrónico

- **Interfaz:** RS-232/449/530/530A/V.35, X.21
- **Protocolo de Enlace de Datos:** HDLC, SLIP
- **Interfaz tipo:** 4 serial
- **Conector:** 25 pin D-Sub (DB-25)
- **Velocidad de transferencia:** 8 Mbps
- **Protocolo de Administración Remota:** SNMP
- **Garantía:** 1 año
- **Número de parte:** HWIC-4T
- **Precio:** \$ 2060,00 + IVA



Figura 4-34: Módulo Cisco 4 puertos seriales

4.1.2.1.6 Cables para Ruteadores

Cable Cisco V.35 DTE

- **Conector izquierdo:** 34 pines M/34 (V.35) macho
- **Conector derecho:** Smart serial 26 pines macho
- **Compatible con tarjetas:** WIC-2T, HWIC-4T
- **Longitud:** 3 m
- **Garantía:** 1 año.
- **Número de parte:** CAB-SS-V35MT
- **Precio:** \$ 82 + IVA



Figura 4-35: Cable Cisco V.35 DTE

Cable Cisco V.35 DCE V.35 – Smart Serial

- **Conector inferior:** 34 pines M/34 (V.35) hembra
- **Conector superior:** *Smart serial* 26 pines macho
- **Compatible con tarjetas:** *WIC-2T, HWIC-4T*
- **Longitud:** 3 m
- **Número de parte:** CAB-SS-V35FC
- **Precio:** \$ 82 + IVA

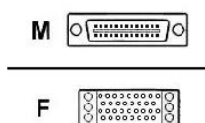


Figura 4-36: Cable Cisco V.35 DCE

Cable Cisco V.35 DCE V.35 H – DB-60 M

- **Conector inferior:** 34 pines M/34 (V.35) hembra
- **Conector superior:** 60 pin *D-Sub* (DB-60) macho
- **Tecnología:** Blindado
- **Longitud:** 3 m
- **Número de parte:** CAB-V35FT
- **Precio:** \$ 72 + IVA

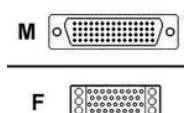


Figura 4-37: Cable Cisco V.35 DB60

Cable Cisco V.35 DCE V.35 M – DB-60 M

- **Conector izquierdo:** 34 pines M/34 (V.35) macho
- **Conector derecho:** 60 pines *D-Sub* (DB-60) macho
- **Longitud:** 3 m
- **Número de parte:** CAB-SS-V35MC
- **Precio:** \$ 72 + IVA

4.1.2.1.7 Access Point

Access Point Cisco Aironet 1242AG

- **Interfaces:** 1 LAN Ethernet 10/100 Base T (PoE) RJ45
- **Antenas:** 2 antenas con conector RP-TNC
- **Método de autenticación:** Secure Shell (SSH), MS-CHAP
- **Estándares compatibles:** 802.11a, 802.11b, 802.3af, 802.11g, 802.1X, 802.11i, Wi-Fi Certificado
- **Protocolo de Enlace de Datos:** 802.11a, 802.11b, 802.11g
- **Velocidad de Transferencia Máxima:** 54 Mbps
- **Algoritmos de Encriptación:** LEAP, AES, WEP de 128 y 40 bits, TLS, PEAP, TTLS, TKIP, WPA, WPA2.
- **Protocolos de Administración Remota:** SNMP, Telnet, HTTP, HTTPS
- **BOOTP:** soportado
- **PoE:** soportado
- **VLAN:** soportado
- **Multi-SSID:** soportado Cisco IOS 12.2(11)
- **Memoria Flash:** 16 MB
- **Memoria RAM:** 32 MB
- **Garantía:** 1 año
- **Número de Parte:** AIR-AP1242AG-A-K9
- **Precio:** \$ 625 + IVA



Figura 4-38: Access Point Cisco Aironet 1242AG

4.1.2.2 Sistema Unificado de Seguridad

Cisco ASA 5510 Servicio Avanzado de Inspección y Prevención de Intrusos

- **Interfaces:** 3 LAN 10/100 Base T, 2 seriales RJ45, 1 administración.
- **Capacidad:** 32000 sesiones concurrentes.
- **Algoritmos de encriptación:** Triple DES, AES.
- **Velocidades:** Firewall: 300 Mbps, Firewall + Anti-x: 150 Mbps, VPN: 170 Mbps.
- **Cantidad de túneles VPN:** 50.
- **Memoria RAM:** 1,28 GB instalado / 1,28 GB máx.
- **Memoria Flash:** 320 MB
- **Garantía:** Lifetime Warranty.
- **Número de parte:** ASA5510-AIP10-K9
- **Precio:** \$ 5175,00 + IVA



Figura 4-39: Sistema de Seguridad Unificado Cisco ASA con módulo IPS

4.1.2.3 Centrales Telefónicas

Cisco Unified Communications Manager Express

Es una solución embebida en el *Software Cisco IOS* que provee de procesamiento de llamadas para Teléfonos *IP Cisco*. Esta solución es posible implementarla en gran variedad de ruteadores *Cisco* de Servicios Integrados y de Acceso Multi-servicio adicionando características de Telefonía *IP*. *Cisco Unified Communications Manager Express* es aconsejable para clientes que busquen bajos costos, confiabilidad, mejorar las características de la solución de telefonía para hasta 240 usuarios.

- **Cisco Call Manager Express Licencia 24 usuarios**
 - Número de parte: FL-CCME-24
 - Precio: \$ 450,00 + IVA
- **Cisco Call Manager Express Licencia 36 usuarios**
 - Número de parte: FL-CCME-36
 - Precio: \$ 660,00 + IVA
- **Cisco Call Manager Express Licencia 48 usuarios**
 - Número de parte: FL-CCME-MEDIUM
 - Precio: \$ 835,00 + IVA

Ruteador <i>CISCO</i>	<i>Cisco Call Manager Express</i> (Teléfonos Máximos)
2801	24
2811	36
2821	48

Tabla 4-1: Ruteadores *Cisco* Serie 2800 usuarios Telefonía *IP*

4.1.2.4 Gateway *IP*

Módulo *Cisco* 4 puertos *FXO*

- **Interfaces:** 4 *FXO RJ11*
- **Slot compatible:** *VIC*
- **Garantía:** 1 año.
- **Número de parte:** *VIC2-4FXO*
- **Precio:** \$ 550,00 + IVA



Figura 4-40: Módulo *Cisco* 4 puertos *FXO*

Módulo *Cisco* 2 puertos FXO

- **Interfaces:** 2 FXO RJ11
- **Slot compatible:** VIC
- **Garantía:** 1 año.
- **Número de parte:** VIC2-2FXO
- **Precio:** \$ 280,00 + IVA



Figura 4-41: Módulo *Cisco* 2 puertos FXO

Módulo *Cisco* 2 puertos FXS

- **Interfaces:** 2 FXS RJ11
- **Slot compatible:** VIC
- **Garantía:** 1 año.
- **Número de parte:** VIC2-2FXS
- **Precio:** \$ 280,00 + IVA



Figura 4-42: Módulo *Cisco* 2 puertos FXS

Módulo *Cisco* 4 puertos FXS/DID

- **Interfaces:** 4 FXS RJ11
- **Slot compatible:** VIC
- **Garantía:** 1 año.
- **Número de parte:** VIC-4FXS/DID
- **Precio:** \$ 560,00 + IVA



Figura 4-43: Módulo Cisco 4 puertos FXS/DID

4.1.2.5 Teléfonos IP

Teléfono IP Cisco 7960G

- **Pantalla:** LCD Monocromática
- **Compatibilidad de Software:** 3.3(3) o superior
- **Asignación de Direcciones IP:** DHCP
- **Principales características:** switch Ethernet integrado.
- **Soporte:** PoE
- **Cantidad de puertos de red:** 2 Ethernet 10/100 Base T
- **Protocolos de red:** TFTP
- **Calidad de Servicio:** IEEE 802.1Q (VLAN)
- **Protocolos de VoIP:** H.323 MGCP, SCCP, SIP.
- **Codecs de Voz:** G.711, G.729a
- **Conexiones:** Headset jack
- **Botones programables:** 6
- **Altavoz incorporado:** Si
- **Garantía:** 1 año
- **Número de parte:** CP-7960G-OPY
- **Precio:** \$ 220,00 + IVA



Figura 4-44: Teléfono IP Cisco 7960G

Teléfono IP Cisco 7942G

- **Pantalla:** LCD Monocromática (320 X 222 píxeles).
- **Asignación de Direcciones IP:** DHCP y estática.
- **Principales características:** Soporte de múltiples protocolos de VoIP, switch Ethernet integrado 2 puertos Ethernet 10/100 Base T PoE.
- **Protocolos de red:** TFTP
- **Calidad de Servicio:** IEEE 802.1Q (VLAN), 802.1p.
- **Seguridad:** AES 128 bits.
- **Protocolos de VoIP:** SCCP, SIP.
- **Codecs de Voz:** G.711, G.722, G.729a, G.729ab, iLBC
- **Características de Voz:** cancelación de eco.
- **Conexiones:** Headset jack
- **Altavoz incorporado:** Si
- **Garantía:** 1 año
- **Número de parte:** CP-7942G
- **Precio:** \$ 305,00 + IVA



Figura 4-45: Teléfono IP Cisco 7942

4.1.2.6 Sistema de Administración de Red

Cisco Works Small Network Management Solution

Cisco Works Small Network Management Solution (SNMS) versión 1.5 es ideal para redes pequeñas. Esta *suite* de aplicaciones de administración brinda un monitoreo básico de la red con dispositivos de múltiples vendedores. *SNMS* permite a los usuarios seleccionar hasta 40 dispositivos *Cisco* para administración avanzada usando herramientas disponibles en esta *suite*.

SNMS facilita a los administradores de red el monitoreo de dispositivos de otras marcas mediante de la administración *SNMP* de *What's Up Gold*. El crecimiento de la red está previsto para esta *suite* ya que brinda una solución de fácil transición y a buen precio al pasar a *Cisco Works LAN Management Solution*, siendo ésta una aplicación que maneja un mayor número de dispositivos y tiene funciones adicionales.

- **Número de Parte:** CWSNM-1.5-K9
- **Precio:** \$ 2160,00 + IVA

4.1.3 VIDEOCONFERENCIA IP⁴⁵

4.1.3.1 DLINK

Videoconferencia DLINK DVC-1000

- **Estándares:** *H.323, H.263, G.711, G.723*
- **Video:** *CIF (352 X 288 pixeles), QCIF (176 X 144 pixeles)*
- **Cuadros por segundo:** Hasta 30
- **Entradas y Salidas:** Poder, Salida de Audio y Video (*RCA*),
- **Conectividad:** 1 puerto *Ethernet 10/100 Base T*, 1 puerto *RJ11* para línea telefónica
- **Cámara:** *Tilt y Focus Manual*
- **Precio:** \$ 170,00 + IVA



Figura 4-46: Equipo DLINK Videoconferencia IP DVC-1000

⁴⁵ Sólo se presenta alternativas de equipos de videoconferencia en marca *DLINK* porque equipos como *Polycom* o *Athera*, están diseñados para utilizar grandes capacidades de transmisión y también tienen un costo muy elevado

Videoconferencia DLINK DVC-1100

- **Estándares:** *H.323, H.263, G.711, G.723*
- **Video:** *CIF (352 X 288 pixeles), QCIF (176 X 144 pixeles)*
- **Cuadros por segundo:** Hasta 30
- **Entradas y Salidas:** Poder, Salida de Audio y Video (*RCA*),
- **Conectividad:** 1 puerto *Ethernet 10/100 Base T RJ45*, Inalámbrica *802.11b 11 Mbps*
- **Cámara:** *Tilt y Focus Manual*
- **Número de parte:** *DVC-1100*
- **Precio:** \$ 250,00 + IVA



Figura 4-47: Equipo **DLINK** Videoconferencia *IP DVC-1100*

4.1.4 EQUIPOS NECESARIOS PARA LAS SUCURSALES Y SUS PRECIOS

Los equipos que se han utilizado para el rediseño de la red son de dos marcas principalmente: *Cisco* y *3COM*. Estas marcas son especializadas en equipos de conectividad. Existen equipos como por ejemplo los de videoconferencia que no existen opciones en estas marcas.

Para los equipos de videoconferencia se ha propuesto equipos *DLINK* que es una marca reconocida a nivel mundial y tiene buenos equipos para videoconferencia. Se proponen dos modelos pero se escogió uno que tiene opciones de conectividad inalámbrica y cableada; esta característica brinda versatilidad a la solución dada la posibilidad de conectarla a la red inalámbrica obteniendo mayor movilidad para conferencias y eventos.

4.1.4.1 Equipos 3COM

4.1.4.1.1 Sucursal Principal (Quito)

Los equipos de conectividad, telefonía IP y seguridad de red necesarios para la sucursal Principal son los que se muestran en la Tabla 4-2.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch 3COM 5500 EI PWR 28 puertos 10/100	3CR17171-91	2050,00	2050,00
1	Switch 3COM 5500 EI PWR 52 puertos 10/100	3CR17172-91	3450,00	3450,00
8	Transceiver 3COM 1000 Base T SFP	3CSFP93	150,00	1200,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM un puerto serial SIC	3C13715	170,00	170,00
1	Cable 3COM V.35 DTE	3C13685	80,00	80,00
1	Sistema Unificado de Seguridad 3COM X5 usuarios ilimitados	3CRTPX5-U-96	1050,00	1050,00
1	Central Telefónica 3COM Asterisk	3CR10551A	1580,00	1580,00
17	Teléfono de Negocios 3COM 3102	3C10402B	210,00	3570,00
17	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	2720,00
5	Teléfono Básico 3COM 3101	3C10401B	140,00	700,00
3	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	2550,00
2	Access Point 3COM 7760 802.11 a/b/g PoE	3CRWE776075	215,00	430,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	20600,00
			IVA 12 %	2472,00
			Total	23072,00

Tabla 4-2: Equipos 3COM Sucursal Principal (Quito)

En la Tabla 4-3 se detallan los modelos de los teléfonos IP por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	8	Teléfono de Negocios 3COM 3102	3C10402B
Ventas	9	Teléfono de Negocios 3COM 3102	3C10402B
Bodega	5	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Crédito	5	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Auditoría Externa	2	Teléfono Básico 3COM 3101	3C10401B
Caja	3	Teléfono Básico 3COM 3101	3C10401B
Contabilidad	3	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Técnico	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Sistemas	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-3: Teléfonos IP 3COM Sucursal Principal (Quito)

4.1.4.1.2 Sucursal Colón (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Colón son los que se muestran en la Tabla 4-4.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch 3COM 5500 <i>EI PWR</i> 28 puertos 10/100	3CR17171-91	2050,00	2050,00
4	Transceiver 3COM 1000 Base <i>T SFP</i>	3CSFP93	150,00	600,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM un puerto serial <i>SIC</i>	3C13715	170,00	170,00
1	Cable 3COM <i>V.35 DTE</i>	3C13685	80,00	80,00
1	Sistema Unificado de Seguridad 3COM X5 25 usuarios	3CRTPX5-25-96	870,00	870,00
1	Central Telefónica 3COM <i>Asterisk</i>	3CR10551A	1580,00	1580,00
9	Teléfono de Negocios 3COM 3102	3C10402B	210,00	1890,00
6	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	960,00
2	Teléfono Básico 3COM 3101	3C10401B	140,00	280,00
2	Gateway <i>IP</i> 3COM 7111 8 puertos <i>FXO</i>	3CRVG71114-07	850,00	1700,00
4	Access Point 3COM 7760 802.11 a/b/g <i>PoE</i>	3CRWE776075	215,00	860,00
2	Videoconferencia <i>DLINK</i> Inalámbrico	DVC-1100	250,00	500,00
			Subtotal	12340,00
			IVA 12 %	1480,80
			Total	13820,80

Tabla 4-4: Equipos 3COM Sucursal Colón (Quito)

En la Tabla 4-5 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos <i>IP</i>			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono de Negocios 3COM 3102	3C10402B
Ventas	7	Teléfono de Negocios 3COM 3102	3C10402B
Bodega	3	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Crédito	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Caja	2	Teléfono Básico 3COM 3101	3C10401B
Técnico	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-5: Teléfonos *IP* 3COM Sucursal Colón (Quito)

4.1.4.1.3 Sucursal CST (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal CST son los que se muestran en la Tabla 4-6.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
2	Switch 3COM 5500 EI PWR 28 puertos	3CR17171-91	2050,00	4100,00
2	Transceiver 3COM 1000 Base T SFP	3CSFP93	150,00	300,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM cuatro puerto serial MIM	3C13764	800,00	800,00
1	Cable 3COM V.35 DTE	3C13685	80,00	80,00
3	Cable 3COM V.35 DCE	3C13686	80,00	240,00
1	Sistema Unificado de Seguridad 3COM X5 25 usuarios	3CRTPX5-25-96	870,00	870,00
1	Central Telefónica 3COM Asterisk	3CR10551A	1580,00	1580,00
9	Teléfono de Negocios 3COM 3102	3C10402B	210,00	1890,00
14	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	2240,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	1700,00
2	Access Point 3COM 7760 802.11 a/b/g PoE	3CRWE776075	215,00	430,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	15280,00
			IVA 12 %	1833,60
			Total	17113,60

Tabla 4-6: Equipos 3COM Sucursal CST (Quito)

En la Tabla 4-7 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono de Negocios 3COM 3102	3C10402B
Garantías	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Mercadeo	7	Teléfono de Negocios 3COM 3102	3C10401SPKRB
Caja	1	Teléfono Básico con Parlante 3COM 3101	3C10401B
Técnico	10	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Sistemas	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-7: Teléfonos IP 3COM Sucursal CST (Quito)

4.1.4.1.4 Sucursal Sur (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Sur de Quito son los que se muestran en la Tabla 4-8.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch 3COM 4500 EI PWR 26 puertos	3CR17571-91	1220,00	1220,00
2	Transceiver 3COM 1000 Base T SFP	3CSFP93	150,00	300,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM un puerto serial SIC	3C13715	170,00	170,00
1	Cable 3COM V.35 DTE	3C13685	80,00	80,00
1	Sistema Unificado de Seguridad 3COM X5 25 Usuarios	3CRTPX5-25-96	870,00	870,00
1	Central Telefónica 3COM Asterisk	3CR10551A	1580,00	1580,00
6	Teléfono de Negocios 3COM 3102	3C10402B	210,00	1260,00
3	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	480,00
2	Teléfono Básico 3COM 3101	3C10401B	140,00	280,00
1	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	850,00
2	Access Point 3COM 7760 802.11 a/b/g PoE	3CRWE776075	215,00	430,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	8570,00
			IVA 12 %	1028,40
			Total	9598,40

Tabla 4-8: Equipos 3COM Sucursal Sur (Quito)

En la Tabla 4-9 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono de Negocios 3COM 3102	3C10402B
Ventas	4	Teléfono de Negocios 3COM 3102	3C10402B
Bodega	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Caja	2	Teléfono Básico 3COM 3101	3C10401B
Técnico	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-9: Teléfonos IP 3COM Sucursal Sur (Quito)

4.1.4.1.5 Sucursal Mayor (Guayaquil)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Mayor son los que se muestran en la Tabla 4-10.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
2	Switch 3COM 5500 EI PWR 28 puertos	3CR17171-91	2050,00	4100,00
2	Transceiver 3COM 1000 Base T SFP	3CSFP93	150,00	300,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM con dos puertos seriales SIC	3C13762	400,00	400,00
2	Cable 3COM V.35 DTE	3C13685	80,00	160,00
1	Sistema Unificado de Seguridad 3COM X5 usuarios ilimitados	3CRTPX5-U-96	1050,00	1050,00
1	Central Telefónica 3COM Asterisk	3CR10551A	1580,00	1580,00
12	Teléfono de Negocios 3COM 3102	3C10402B	210,00	2520,00
9	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	1440,00
2	Teléfono Básico 3COM 3101	3C10401B	140,00	280,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	1700,00
2	Access Point 3COM 7760 802.11 a/b/g PoE	3CRWE776075	215,00	430,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	15010,00
			IVA 12 %	1801,20
			Total	16811,20

Tabla 4-10: Equipos 3COM Sucursal Mayor (Guayaquil)

En la Tabla 4-11 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	3	Teléfono de Negocios 3COM 3102	3C10402B
Ventas	7	Teléfono de Negocios 3COM 3102	3C10402B
Bodega	4	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Crédito	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Mercadeo	2	Teléfono de Negocios 3COM 3102	3C10402B
Caja	2	Teléfono Básico 3COM 3101	3C10401B
Contabilidad	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Técnico	3	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-11: Teléfonos IP 3COM Sucursal Mayor (Guayaquil)

4.1.4.1.6 Sucursal Sur (Guayaquil)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Sur de Guayaquil son los que se muestran en la Tabla 4-12.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch 3COM 4500 EI PWR 26 puertos	3CR17571-91	1220,00	1220,00
2	Transceiver 3COM 1000 Base T SFP	3CSFP93	150,00	300,00
1	Ruteador 3COM 5012	3C13701	800,00	800,00
1	Tarjeta 3COM un puerto serial SIC	3C13715	170,00	170,00
1	Cable 3COM V.35 DTE	3C13686	80,00	80,00
1	Sistema Unificado de Seguridad 3COM X5 25 usuarios	3CRTPX5-U-96	870,00	870,00
1	Central Telefónica 3COM Asterisk	3CR10551A	1580,00	1580,00
5	Teléfono de Negocios 3COM 3102	3C10402B	210,00	1050,00
3	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB	160,00	480,00
1	Teléfono Básico 3COM 3101	3C10401B	140,00	140,00
1	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	850,00
1	Access Point 3COM 7760 802.11 a/b/g PoE	3CRWE776075	215,00	215,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	8005,00
			IVA 12 %	960,60
			Total	8965,60

Tabla 4-12: Equipos 3COM Sucursal Sur (Guayaquil)

En la Tabla 4-13 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono de Negocios 3COM 3102	3C10402B
Ventas	3	Teléfono de Negocios 3COM 3102	3C10402B
Bodega	2	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB
Caja	1	Teléfono Básico 3COM 3101	3C10401B
Técnico	1	Teléfono Básico con Parlante 3COM 3101	3C10401SPKRB

Tabla 4-13: Teléfonos IP 3COM Sucursal Sur (Guayaquil)

4.1.4.2 Equipos Cisco

4.1.4.2.1 Sucursal Principal (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Principal son los que se muestran en la Tabla 4-14.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	3500,00
1	Switch Cisco 3750 48PS-S PoE 48 puertos 10/100	WS-C3750-48PS-S	6150,00	6150,00
8	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	2400,00
2	Cable Cisco StackWise 50 cm	CAB-STACK-50CM-NH	122,00	244,00
1	Ruteador Cisco 2821 Voice Bundle (48 extensiones)	C2821-CCME/K9	3440,00	3440,00
1	Tarjeta Cisco un puerto serial WIC	WIC-1T	310,00	310,00
1	Cable Cisco V.35 DTE DB-60	CAB-V35FT	72,00	72,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
17	Teléfono Cisco IP 7942G	CP-7942G	305,00	5185,00
22	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	4840,00
3	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	2550,00
2	Access Point Cisco Aironet 1242AG 802.11 a/g PoE	AIR-AP1242AG-A-K9	625,00	625,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	34741,00
			IVA 12 %	4168,92
			Total	38909,92

Tabla 4-14: Equipos Cisco Sucursal Principal (Quito)

En la Tabla 4-15 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	8	Teléfono Cisco IP 7942G	CP-7942G
Ventas	9	Teléfono Cisco IP 7942G	CP-7942G
Bodega	5	Teléfono Cisco IP 7960G	CP-7960G-OPY
Crédito	5	Teléfono Cisco IP 7960G	CP-7960G-OPY
Auditoría Externa	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Caja	3	Teléfono Cisco IP 7960G	CP-7960G-OPY
Contabilidad	3	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Sistemas	2	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-15: Teléfonos IP Cisco Sucursal Principal (Quito)

4.1.4.2.2 Sucursal Colón (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Colón son los que se muestran en la Tabla 4-16.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	3500,00
4	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	1200,00
1	Ruteador Cisco 2801 Voice Bundle (24 extensiones)	CISCO2801-CCME/K9	2170,00	2170,00
1	Tarjeta Cisco un puerto serial WIC	WIC-1T	310,00	310,00
1	Cable Cisco V.35 DTE DB-60	CAB-V35FT	72,00	72,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
9	Teléfono Cisco IP 7942G	CP-7942G	305,00	2745,00
8	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	1760,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	1700,00
4	Access Point Cisco Aironet 1242AG 802.11 a/b/g PoE	AIR-AP1242AG-A-K9	625,00	1250,00
2	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	500,00
			Subtotal	20382,00
			IVA 12 %	2445,84
			Total	22827,84

Tabla 4-16: Equipos Cisco Sucursal Colón (Quito)

En la Tabla 4-17 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono Cisco IP 7942G	CP-7942G
Ventas	7	Teléfono Cisco IP 7942G	CP-7942G
Bodega	3	Teléfono Cisco IP 7960G	CP-7960G-OPY
Crédito	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Caja	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	1	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-17: Teléfonos IP Cisco Sucursal Colón (Quito)

4.1.4.2.3 Sucursal CST (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal CST son los que se muestran en la Tabla 4-18.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
2	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	7000,00
2	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	600,00
2	Cable Cisco StackWise 50 cm	CAB-STACK-50CM-NH	122,00	244,00
1	Ruteador Cisco 2811 Voice Bundle (36 extensiones)	C2811-CCME/K9	2360,00	2360,00
1	Tarjeta Cisco cuatro puertos seriales HWIC	HWIC-4T	2060,00	2060,00
1	Cable Cisco V.35 DTE Smart Serial	CAB-SS-V35MT	82,00	82,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
2	Teléfono Cisco IP 7942G	CP-7942G	305,00	610,00
21	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	4620,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	550,00	1100,00
2	Access Point Cisco Aironet 1242AG 802.11 a/g PoE	AIR-AP1242AG-A-K9	625,00	625,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	24726,00
			IVA 12 %	2967,12
			Total	27693,12

Tabla 4-18: Equipos Cisco Sucursal CST (Quito)

En la Tabla 4-19 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos <i>IP</i>			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono Cisco IP 7942G	CP-7942G
Garantías	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Mercadeo	7	Teléfono Cisco IP 7960G	CP-7960G-OPY
Caja	1	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	10	Teléfono Cisco IP 7960G	CP-7960G-OPY
Sistemas	1	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-19: Teléfonos *IP* Cisco Sucursal CST (Quito)

4.1.4.2.4 Sucursal Sur (Quito)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Sur de Quito son los que se muestran en la Tabla 4-20.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	3500,00
2	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	600,00
1	Ruteador Cisco 2801 Voice Bundle (24 extensiones)	CISCO2801-CCME/K9	2170,00	2170,00
1	Tarjeta Cisco un puerto serial WIC	WIC-1T	310,00	310,00
1	Cable Cisco V.35 DTE DB-60	CAB-V35FT	72,00	72,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
6	Teléfono Cisco IP 7942G	CP-7942G	305,00	1830,00
5	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	1100,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	1700,00
2	Access Point Cisco Aironet 1242AG 802.11 a/g PoE	AIR-AP1242AG-A-K9	625,00	625,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	17332,00
			IVA 12 %	2079,84
			Total	19411,84

Tabla 4-20: Equipos Cisco Sucursal Sur (Quito)

En la Tabla 4-21 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos IP			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono Cisco IP 7942G	CP-7942G
Ventas	4	Teléfono Cisco IP 7942G	CP-7942G
Bodega	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Caja	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	1	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-21: Teléfonos IP Cisco Sucursal Sur (Quito)

4.1.4.2.5 Sucursal Mayor (Guayaquil)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Mayor son los que se muestran en la Tabla 4-22.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
2	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	7000,00
8	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	2400,00
2	Cable Cisco StackWise 50 cm	CAB-STACK-50CM-NH	122,00	244,00
1	Ruteador Cisco 2811 Voice Bundle (36 extensiones)	C2811-CCME/K9	2360,00	2360,00
1	Tarjeta Cisco dos puertos seriales WIC	WIC-2T	530,00	530,00
2	Cable Cisco V.35 DTE Smart Serial	CAB-SS-V35MT	82,00	164,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
12	Teléfono Cisco IP 7942G	CP-7942G	305,00	3660,00
11	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	2420,00
2	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	1700,00
2	Access Point Cisco Aironet 1242AG 802.11 a/g PoE	AIR-AP1242AG-A-K9	625,00	625,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	26528,00
			IVA 12 %	3183,36
			Total	29711,36

Tabla 4-22: Equipos Cisco Sucursal Mayor (Guayaquil)

En la Tabla 4-23 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos <i>IP</i>			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	3	Teléfono Cisco IP 7942G	CP-7942G
Ventas	7	Teléfono Cisco IP 7942G	CP-7942G
Bodega	4	Teléfono Cisco IP 7960G	CP-7960G-OPY
Crédito	1	Teléfono Cisco IP 7960G	CP-7960G-OPY
Mercadeo	2	Teléfono Cisco IP 7942G	CP-7960G-OPY
Caja	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Contabilidad	1	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	3	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-23: Teléfonos *IP* Cisco Sucursal Mayor (Guayaquil)

4.1.4.2.6 Sucursal Sur (Guayaquil)

Los equipos de conectividad, telefonía *IP* y seguridad de red necesarios para la Sucursal Sur son los que se muestran en la Tabla 4-24.

Cantidad	Ítem	Número de Parte	Precio Unitario	Precio Total
1	Switch Cisco 3750 24PS-S PoE 24 puertos 10/100	WS-C3750-24PS-S	3500,00	3500,00
2	Transceiver Cisco 1000 Base T SFP	GLC-T	300,00	600,00
1	Ruteador Cisco 2801 Voice Bundle (24 extensiones)	CISCO2801-CCME/K9	2170,00	2170,00
1	Tarjeta Cisco un puerto serial WIC	WIC-1T	310,00	310,00
1	Cable Cisco V.35 DTE DB-60	CAB-V35FT	72,00	72,00
1	Cisco ASA 5510 IPS	ASA5510-AIP10-K9	5175,00	5175,00
5	Teléfono Cisco IP 7942G	CP-7942G	305,00	1525,00
4	Teléfono Cisco IP 7960G	CP-7960G-OPY	220,00	880,00
1	Gateway IP 3COM 7111 8 puertos FXO	3CRVG71114-07	850,00	850,00
1	Access Point Cisco Aironet 1242AG 802.11 a/b/g PoE	AIR-AP1242AG-A-K9	625,00	625,00
1	Videoconferencia DLINK Inalámbrico	DVC-1100	250,00	250,00
			Subtotal	15957,00
			IVA 12 %	1914,84
			Total	17871,84

Tabla 4-24: Equipos Cisco Sucursal Sur (Guayaquil)

En la Tabla 4-25 se detallan los modelos de los teléfonos *IP* por departamento.

Teléfonos <i>IP</i>			
Departamento	Teléfonos	Modelo de los Teléfonos	Número de Parte
Administrativo	2	Teléfono Cisco IP 7942G	CP-7942G
Ventas	3	Teléfono Cisco IP 7942G	CP-7942G
Bodega	2	Teléfono Cisco IP 7960G	CP-7960G-OPY
Caja	1	Teléfono Cisco IP 7960G	CP-7960G-OPY
Técnico	1	Teléfono Cisco IP 7960G	CP-7960G-OPY

Tabla 4-25: Teléfonos *IP* Cisco Sucursal Sur (Guayaquil)

4.1.5 SOLUCIONES PARA INTERCONEXIÓN DE SUCURSALES

4.1.5.1 *Telconet*⁴⁶

4.1.5.1.1 *Enlaces de Datos*

Enlace Nacional Quito – Guayaquil

- **Backbone:** Cisco IP- MPLS 10 Gbps
- **Soporte técnico:** 7 X 24 X 365
- **Tiempo de respuesta ante fallas:** Inmediato, mediante contacto telefónico. Máximo dos horas, en caso de rotura de fibra óptica.
- **Supervisión técnica y administración del enlace:** 7 X 24 X 365
- **Equipo de respaldo:** equipos microonda con la finalidad de solventar cualquier desperfecto en un máximo de 2 horas.
- **Nivel de compresión:** 1:1 (no se comprime)
- **Número de usuarios:** Ilimitados
- **Ampliación de Capacidad de transmisión:** hasta 100 Mbps de última milla.
- **Tecnología de última milla:** *Telconet* dispone de una Red de Área Metropolitana de fibra óptica con tecnología *Gigabit Ethernet*.
- **Monitoreo del Enlace:** mediante el sistema *CACTI*
- **Garantía de funcionamiento:** 99,5 % garantizado, 0,05% es el tiempo sin servicio y mantenimiento de última milla.
- **Capacidad:** 1024 Kbps
- **Precio Mensual:** \$ 600 + IVA
- **Costo de Instalación:** \$ 300 + IVA

⁴⁶ Datos obtenidos de la cotización enviada por Ramiro Naranjo de *Telconet*

Enlace Local Guayaquil

- **Backbone:** Cisco IP- MPLS 10 Gbps
- **Soporte técnico:** 7 X 24 X 365
- **Tiempo de respuesta ante fallas:** Inmediato, mediante contacto telefónico. Máximo dos horas, en caso de rotura de fibra óptica.
- **Supervisión técnica y administración del enlace:** 7 X 24 X 365
- **Equipo de respaldo:** equipos microonda con la finalidad de solventar cualquier desperfecto en un máximo de 2 horas.
- **Nivel de compresión:** 1:1 (no se comprime)
- **Número de usuarios:** Ilimitados
- **Ampliación de Capacidad de transmisión:** hasta 100 Mbps de última milla.
- **Tecnología de última milla:** Telconet dispone de una Red de Área Metropolitana de fibra óptica con tecnología *Gigabit Ethernet*.
- **Monitoreo del Enlace:** mediante el sistema *CACTI*
- **Garantía de funcionamiento:** 99,5 % garantizado, 0,05% es el tiempo sin servicio y mantenimiento de última milla.
- **Opción 1:**
 - **Capacidad:** 512 Kbps
 - **Precio Mensual:** \$ 220 + IVA
- **Opción 2:**
 - **Capacidad:** 1024 Kbps
 - **Precio Mensual:** \$ 290 + IVA
- **Costo de Instalación:** \$ 300 + IVA

Servicio de *Internet* Corporativo

- **Capacidad de *Internet* para la salida Internacional:** 6 STM-1 (930 Mbps)

- **Servicio y soporte técnico:** 7 X 24 X 365
- **Tiempo de respuesta ante fallas de conexión:** Inmediato, mediante contacto telefónico. Máximo dos horas, en caso de rotura de la fibra óptica.
- **Equipo de respaldo:** equipos microonda con la finalidad de solventar cualquier desperfecto en un máximo de 2 horas.
- **Compresión del canal:** 1:1
- **Direcciones IP Públicas:** Las requeridas por el cliente previa verificación.
- **Enlace principal de FO que dispone Telconet desde Quito:** FO Transnexa hasta el NAP de las Américas en Florida – USA. Disponibilidad 99.9%
- **Enlace de respaldo de FO que dispone Telconet en Quito:**
 - FO del Cable Panamericano hasta el NAP de las Américas en Florida – USA. Disponibilidad: 99.9%
 - FO de Emergia hasta el NAP de las Américas en Florida – USA. Disponibilidad: 99.9%
- **Tiempo de Latencia:** Dentro del *backbone* local 1 ms. Internacional, 100 ms al NAP.
- **Tecnología de última milla:** Fibra Óptica con infraestructura propia de Telconet.
- **Monitoreo del Enlace:** Vía Web usando el sistema CACTI
- **Garantía de Funcionamiento:** 99,6 %, el 0,04% incluye tiempo sin servicio y mantenimiento de última milla.
- **Enlaces de Respaldo:** Dos cuentas *Dial-UP*
- **Opción 1:**
 - **Capacidad de transmisión:** 2048 Kbps
 - **Precio:** \$ 1200 + IVA (mensualmente)
- **Opción 2:**
 - **Capacidad de transmisión:** 1024 Kbps
 - **Precio:** \$ 650 + IVA (mensualmente)
- **Costo de instalación:** \$ 300 + IVA

4.1.5.2 PuntoNet⁴⁷

Enlace Nacional Quito – Guayaquil

- **Tecnología de última milla:** enlace de radio con tecnología *Wimax*.
- **Frecuencia de operación:** 5.4 a 5.7 GHz.
- **Backbone:** *IP-MPLS*
- **Compartición:** 1:1
- **Capacidad Máxima:** hasta 25 Mbps full dúplex.
- **Manejo de interferencias:** incrementando la potencia, cambio de polarización, intercambio de canales, cambio de modulación.
- **Características:** *bridging* y *routing*, modulación *OFDM*, división de frecuencias para polarización horizontal o vertical.
- **Soporte:** *VLANs* y *QoS* extremo a extremo.
- **Administración del enlace:** local y remota basada en *SNMP*, con ambiente gráfico.
- **Antenas:** que reducen el ruido ocasionado por el movimiento o por cambios bruscos de temperatura, porque las antenas están hechas de materiales aislantes que minimizan estos efectos.
- **Soporte y monitoreo de la red:** 7 X 24 X 365
- **Tiempo de respuesta ante fallas:** 2 horas
- **Capacitación:** 2 horas al responsable de la red del cliente.
- **Servicio Garantizado última milla:** 99,6 % anual
- **Costo de instalación:** \$ 100,00 + IVA (una sola vez)
- **Opción 1:**
 - **Capacidad:** 512 Kbps
 - **Precio:** \$ 260,00 + IVA (mensualmente)
- **Opción 2:**
 - **Capacidad:** 1024 Kbps
 - **Precio:** \$ 497,00 + IVA (mensualmente)

⁴⁷ Datos obtenidos de la Cotización enviada por Claudia Vega Punto Net.

Enlace Local Guayaquil

- **Tecnología de última milla:** enlace de radio con tecnología *Wimax*.
- **Frecuencia de operación:** 5.4 a 5.7 GHz.
- **Backbone:** *IP-MPLS*
- **Compartición:** 1:1
- **Capacidad Máxima:** hasta 25 Mbps full dúplex.
- **Manejo de interferencias:** incrementando la potencia, cambio de polarización, intercambio de canales, cambio de modulación.
- **Características:** *bridging* y *routing*, modulación *OFDM*, división de frecuencias para polarización horizontal o vertical.
- **Soporte:** *VLANs* y *QoS* extremo a extremo.
- **Administración del enlace:** local y remota basada en *SNMP*, con ambiente gráfico.
- **Antenas:** que reducen el ruido ocasionado por el movimiento o por cambios bruscos de temperatura, porque las antenas están hechas de materiales aislantes que minimizan estos efectos.
- **Soporte y monitoreo de la red:** 7 X 24 X 365
- **Tiempo de respuesta ante fallas:** 2 horas
- **Capacitación:** 2 horas al responsable de la red del cliente.
- **Servicio Garantizado última milla:** 99,6 % anual
- **Costo de instalación:** \$ 100,00 + IVA (una sola vez)
- **Opción 1:**
 - **Capacidad:** 512 Kbps
 - **Precio:** \$ 180,00 + IVA (mensualmente)
- **Opción 2:**
 - **Capacidad:** 1 Mbps
 - **Precio:** \$ 250,00 + IVA (mensualmente)

Acceso a Internet

- **Tecnología de última milla:** enlace de radio con tecnología *Wimax*.
- **Frecuencia de operación:** 5.4 a 5.7 GHz.

- **Backbone:** *IP-MPLS*
- **Compartición:** 1:1
- **Capacidad Máxima:** hasta 25 *Mbps full dúplex*.
- **Manejo de interferencias:** incrementando la potencia, cambio de polarización, intercambio de canales, cambio de modulación.
- **Características:** *bridging* y *routing*, modulación *OFDM*, división de frecuencias para polarización horizontal o vertical.
- **Soporte:** *VLANs* y *QoS* extremo a extremo.
- **Administración del enlace:** local y remota basada en *SNMP*, con ambiente gráfico.
- **Antenas:** que reducen el ruido ocasionado por el movimiento o por cambios bruscos de temperatura, porque las antenas están hechas de materiales aislantes que minimizan estos efectos.
- **Enlace principal de FO que dispone Punto Net desde Quito:** *FO Transnexa* hasta el *NAP* de las Américas en *Florida – USA*. Disponibilidad 99.9%
- **Enlace de respaldo de FO que dispone Punto Net en Quito:** *FO Andinadatos* hasta el *NAP* de las Américas en *Florida – USA*. Disponibilidad 99.9%
- **Tiempo de respuesta ante fallas:** 2 horas
- **Soporte y monitoreo de la red:** 7 X 24 X 365
- **Direcciones IP:** Asignación 4 direcciones *IP* públicas
- **Capacitación:** 2 horas al responsable de la red del cliente.
- **Servicio Garantizado última milla:** 99,6 % anual
- **Costo de instalación:** \$ 100,00 + IVA (una sola vez)
- **Opción 1:**
 - **Capacidad:** 1024 *Kbps*
 - **Precio:** \$ 700,00 + IVA (mensualmente)
- **Opción 2:**
 - **Capacidad:** 2048 *Kbps*
 - **Precio:** \$ 1100,00 + IVA (mensualmente)

4.1.5.3 Resumen y Elección de Alternativa del Servicio

4.1.5.3.1 Enlace Nacional Sucursal CST (Quito) – Sucursal Mayor (Guayaquil)

Característica	Telconet	Punto Net
Tecnología de Última Milla	Fibra Óptica	Wimax
Backbone	IP-MPLS	IP-MPLS
Frecuencia de Operación	N.A.	5.4 a 5.7 GHz
Compartición	1:1	1:1
Capacidad Máxima de Última Milla	100 Mbps	25 Mbps
Soporte	7 X 24 X 365	7 X 24 X 365
Tiempo de respuesta ante fallas de conexión	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica, se instala un equipo de microondas de reemplazo (última milla)	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica de backbone
SLA	99,6 % anual	99,6 % anual
Costo Instalación	\$ 300 (una sola vez)	\$ 100 (una sola vez)
Capacidad (Opción 1)	512 Kbps	512 Kbps
Costo Servicio (Opción 1)	\$ 350 (mensual)	\$ 260 (mensual)
Capacidad (Opción 2)	1 Mbps	1 Mbps
Costo Servicio (Opción 2)	\$ 600 (mensual)	\$ 497 (mensual)

Tabla 4-26: Características y Costos del Enlace Nacional Quito – Guayaquil

4.1.5.3.2 Enlace Local Sucursales de Guayaquil

Característica	Telconet	Punto Net
Tecnología de Última Milla	Fibra Óptica	Wimax
Backbone	IP-MPLS	IP-MPLS
Frecuencia de Operación	N.A.	5.4 a 5.7 GHz
Compartición	1:1	1:1
Capacidad Máxima de Última Milla	100 Mbps	25 Mbps
Soporte	7 X 24 X 365	7 X 24 X 365
Tiempo de respuesta ante fallas de conexión	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica, se instala un equipo de microondas de reemplazo (última milla)	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica de backbone
SLA	99,6 % anual	99,6 % anual
Costo Instalación	\$ 300 (una sola vez)	\$ 100 (una sola vez)
Capacidad (Opción 1)	512 Kbps	512 Kbps
Costo Servicio (Opción 1)	\$ 220 (mensual)	\$ 180 (mensual)
Capacidad (Opción 2)	1 Mbps	1 Mbps
Costo Servicio (Opción 2)	\$ 290 (mensual)	\$ 250 (mensual)

Tabla 4-27: Características y Costos del Enlace Local Sucursales de Guayaquil

4.1.5.3.3 Servicio de Internet

Característica	Telconet	Punto Net
Tecnología de Última Milla	Fibra Óptica	Wimax
Frecuencia de Operación	N.A.	5.4 a 5.7 GHz
Compartición	1:1	1:1
Capacidad Máxima de Última Milla	100 Mbps	25 Mbps
Soporte	7 X 24 X 365	7 X 24 X 365
Tiempo de respuesta ante fallas de conexión	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica, se instala un equipo de microondas de reemplazo (última milla)	Inmediato mediante contacto telefónico y 2 horas en caso de fallas en la fibra óptica de <i>backbone</i>
SLA	99,6 % anual	99,6 % anual
Direcciones IP Públicas	Las requeridas por el cliente previa verificación	4
Enlace de Respaldo	2 cuentas <i>Dial UP</i>	2 cuentas <i>Dial UP</i>
Costo Instalación	\$ 300 (una sola vez)	\$ 100 (una sola vez)
Capacidad (Opción 1)	1 Mbps	1 Mbps
Costo Servicio (Opción 1)	\$ 650 (mensual)	\$ 700 (mensual)
Capacidad (Opción 2)	2 Mbps	2 Mbps
Costo Servicio (Opción 2)	\$ 1200 (mensual)	\$ 1100 (mensual)

Tabla 4-28: Características y Costos del Servicio de Internet

4.1.5.3.4 Elección del Servicio de Internet y Enlaces entre Sucursales

Telconet ofrece una solución con fibra óptica hasta las oficinas del cliente y en caso de fallos, se instalará equipos microonda de reemplazo incrementando los tiempos de solución de problemas a más de dos horas como indica el proveedor, si se tiene inconvenientes al instalar los equipos de microonda. Por lo que esta solución dejaría más tiempo sin servicio a la empresa si existe un corte de la fibra.

La solución escogida como la mejor entre los dos proveedores de Internet y enlaces entre las sucursales es Punto Net, porque proponen una solución con la última milla con tecnología WIMAX. Su montaje y desmontaje es fácil y práctico por lo que permite obtener mejores tiempos de respuesta ante fallas de equipos (2 horas), si se lo compara con estructuras como la fibra óptica que toma tiempos altos para la solución de problemas, hasta días para su reparación o reinstalación dado un corte en la fibra óptica. Adicionalmente Punto Net tiene costos de instalación y de servicio más bajos que Telconet, pero tiene características similares en los servicios propuestos.

Los servicios a contratarse con Punto Net son:

- Conexión a *Internet* para Quito: 2 *Mbps* con una mensualidad de US \$ 1100 y un costo de instalación de US \$ 100 por una sola vez.
- Conexión a *Internet* para Guayaquil: 1 *Mbps* con una mensualidad de US \$ 700 y un costo de instalación de US \$ 100 por una vez.
- Enlace Quito – Guayaquil: 512 *Kbps* con una mensualidad de US \$260, no se tiene costo de instalación ya que ocuparía el mismo ruteador para *Internet* y Datos.
- Enlace Sucursal Mayor Guayaquil: 512 *Kbps* con una mensualidad de US \$ 180 y un costo de instalación de US \$ 100 por sola vez.

Durante el primer mes de uso de los servicios se monitoreará los enlaces y la salida a *Internet* de Quito y Guayaquil, para según este análisis solicitar el incremento de la capacidad de los canales que así lo requieran. Un ruteador en cada sucursal manejará el enlace de datos y el servicio de *Internet*.

4.2 ANÁLISIS COSTO / BENEFICIO

Para el rediseño de la red se han utilizado equipos de dos marcas principalmente: *Cisco* y *3COM*. Estas marcas son las más utilizadas en equipos de conectividad a nivel empresarial. Las dos opciones cumplen con las características detalladas en los requisitos de los equipos de la red.

Cada marca tiene características propias que dan un valor agregado a sus clientes, pero los equipos cumplen con las características del diseño realizado para este proyecto. Razón por la cual se toman las dos soluciones como equivalentes para el Análisis Costo / Beneficio, y se determinará el costo total del proyecto con las dos marcas para obtener la rentabilidad de cada solución. La solución más rentable en un horizonte de 5 años, se sugerirá como la más indicada para su implementación.

Dentro de los costos no se tomó en cuenta los costos diseño y la implementación del cableado estructurado, lo cual es muy importante pero esta fuera del alcance de este proyecto.

4.2.1 COSTOS DE INVERSIÓN

Los costos de inversión de cada solución, contempla el pago de rubros adicionales como son: diseño del proyecto, costo de instalación y configuración de equipos, costos de instalación de los enlaces e *Internet*. Estos costos se presentan a continuación por solución:

Solución 1

Solución 1 (Equipos 3COM)	
Sucursal	Precio US \$
Sucursal Principal (Quito)	20.600,00
Sucursal Colón (Quito)	12.340,00
Sucursal CST (Quito)	15.280,00
Sucursal Sur (Quito)	8.570,00
Sucursal Mayor (Guayaquil)	15.010,00
Sucursal Sur (Guayaquil)	8.005,00
TOTAL	79.805,00

Tabla 4-29: Costos de Equipos 3COM por Sucursales

Servicio	Capacidad de Transmisión	Costo de Instalación US \$
<i>Internet</i> Quito	2048 Kbps	100,00
<i>Internet</i> Guayaquil	1024 Kbps	100,00
Enlace Quito – Guayaquil	512 Kbps	0,00
Enlace Local Guayaquil	512 Kbps	100,00

Tabla 4-30: Costos de Instalación enlaces de Datos e *Internet*

Rubro	Precios US \$
Equipos	79.805,00
Diseño del proyecto	12.000,00
Instalación y configuración de equipos	5.000,00
Instalación de enlaces	100,00
Instalación de <i>Internet</i>	200,00
TOTAL	97.105,00

Tabla 4-31: Costos Solución 1 (Equipos 3COM)

Solución 2

Solución 2 (Equipos Cisco)	
Sucursal	Precio US \$
Sucursal Principal (Quito)	34.741,00
Sucursal Colón (Quito)	20.382,00
Sucursal CST (Quito)	24.726,00
Sucursal Sur (Quito)	17.332,00
Sucursal Mayor (Guayaquil)	26.528,00
Sucursal Sur (Guayaquil)	15.957,00
TOTAL	139.666,00

Tabla 4-32: Costos de Equipos Cisco por Sucursales

Rubro	Precios US \$
Equipos	139.666,00
Diseño del proyecto	12.000,00
Instalación y configuración de equipos	5.000,00
Instalación de enlaces	100,00
Instalación de <i>Internet</i>	200,00
TOTAL	156.966,00

Tabla 4-33: Costos Solución 2 (Equipos Cisco)

4.2.2 COSTOS DE OPERACIÓN

Los costos incrementales de operación de las soluciones que constan durante su vida útil, se estimaron a base de los pagos por: *Internet* y enlaces entre sucursales que se pagan mensualmente, pero son considerados como anuales para el análisis. Adicionalmente, se debe tomar en cuenta los costos de las vacunas digitales de los *firewall* e *IPS* de *Cisco* o *3COM*, según la solución escogida.

En estos costos incrementales no se consideró los pagos a los técnicos, electricidad entre otros debido a que éstos ya constan en los pagos de la empresa.

Servicio	Capacidad de Transmisión	Costo Mensual	Costo Anual
Internet Quito 1:1	2048 Kbps	1.100,00	13.200,00
Internet Guayaquil 1:1	1024 Kbps	700,00	8.400,00
Enlace Quito – Guayaquil 1:1	512 Kbps	260,00	3.120,00
Enlace Local Guayaquil	512 Kbps	180,00	2.160,00
Vacuna Digital Firewall / IPS			3360,00
TOTAL			30.240,00

Tabla 4-34: Costos Operativos y de Mantenimiento

El monto anual promedio de estos costos es de US \$ 30,240.00, que es el resultado de sumar los costos mensuales de los enlaces entre sucursales contratados y el servicio de *Internet*.

4.2.3 ESTIMACIÓN DE BENEFICIOS

Para calcular los beneficios del proyecto, se estimaron incrementos de ventas del 0,25% que son conservadores al contar con una nueva infraestructura de red y comunicaciones. Algunos beneficios del proyecto son:

- Incrementar la disponibilidad de los sistemas de la empresa
- Optimizar los recursos en las comunicaciones entre las sucursales
- Incrementar la productividad de los empleados con una infraestructura de red eficiente y segura, entre los beneficios más relevantes.

Supuestos con Proyecto	Supuestos	Ventas Netas Estimadas	% Incremento	Reducción de Gastos	Totales
Incremento en Ventas	0,25 %	28.863.091,14	72.157,73		28.935.248,87
Disminución en costos de telefonía	20 %	50.000,00		10.000,00	40.000,00
Disminución en sueldos, salarios y demás remuneraciones	2 %	137.751,28		2.755,03	134.996,25
Disminución en aportes a la Seguridad Social	2 %	23.634,10		472,68	23.161,42
Disminución en mantenimiento y reparaciones	15 %	33.408,10		5.011,22	28.396,89
TOTALES		29.107.884,62	72.157,73	18.238,92	29.161.803,43

Tabla 4-35: Estimación de Beneficios del Proyecto

Además se consideró reducción de gastos utilizando la metodología de liberación de recursos, analizando los gastos que se reducirían con la implementación de este proyecto.

La liberación de recursos se ha realizado en:

- Disminución de costos de telefonía tradicional dada la implementación de telefonía *IP* y el uso de los enlaces entre sucursales para llamadas internas y para llamadas internacionales mediante *Internet*.
- Disminución en sueldos, salarios y demás remuneraciones; la implementación de una infraestructura robusta y administrada por un sistema de administración de red, que incluye la parte de telefonía *IP* disminuye el tiempo de solución de problemas y los costos de horas extras de los empleados existentes.
- Disminución de aportes a la Seguridad Social, dada la disminución de horas extras por trabajos emergentes en consecuencia de fallos en la infraestructura de redes y telefonía.
- Disminución en mantenimiento y reparaciones, al tener una sola red para voz, datos y video se ahorra en infraestructura, en consecuencia mantenimiento y reparaciones. Antes para la red de telefonía se debía tener un técnico y para la red de datos otro, estos costos se disminuyen al implementar redes convergentes.

Adicionalmente, en la proyección de los beneficios se ha considerado los siguientes supuestos:

- Un crecimiento en ventas del 2,4% (crecimiento histórico que mantiene las ventas de la empresa), y;
- La liberación de recursos crecen a la inflación promedia anual al 3,3%.

Años	Incremento en Ventas	Liberación de Recursos⁴⁸	Beneficio Neto
1	72.157,73	18.238,92	90.396,65
2	73.889,51	18.848,81	92.730,32
3	75.662,86	19.462,55	95.125,42
4	77.478,11	20.104,82	97.583,59
5	79.338,26	20.768,28	100.106,54

Tabla 4-36: Estimación de Beneficios

⁴⁸ Por reducción de gasto

4.2.4 IMPACTO DEL PROYECTO

Como impactos adicionales del proyecto se pueden señalar los siguientes:

- Seguridad de la información;
- Incremento en la productividad;
- Incremento de la disponibilidad de la red;
- Mejoramiento de las comunicaciones tanto internas como externas;
- Disminución de costos operativos; entre otros.

Los resultados del costo beneficio son los siguientes:

- Solución 1

Años	Inversión	Costo Operación y Mantenimiento Total	Beneficios	Flujo Neto
0	97.105,00			(97.105,00)
1		30.240,00	90.396,65	60.156,65
2		30.240,00	92.730,32	62.490,32
3	24.276,25	30.240,00	95.125,42	40.609,17
4		30.240,00	97.583,59	67.343,59
5		30.240,00	100.106,54	69.866,54
VAN	118.780,22	109.008,43	341.163,00	117.770,22
TIR				53,62 %

Tabla 4-37: Resultados Análisis Costo/Beneficio Solución 1

- Solución 2

Años	Inversión	Costos de Operación y Mantenimiento Totales	Beneficios	Flujo Neto
0	156.966,00			(156.966,00)
1		30.240,00	90.396,65	60.156,65
2		30.240,00	92.730,32	62.490,32
3	39.241,50	30.240,00	95.125,42	25.643,92
4		30.240,00	97.583,59	67.343,59
5		30.240,00	100.106,54	69.866,54
VAN	192.003,05	109.008,43	341.163,00	47.257,25
TIR				23,38 %

Tabla 4-38: Resultados Análisis Costo/Beneficio Solución 2

Como dato para calcular el TIR se ha tomado una tasa de descuento del 12% que es la que se maneja en el Banco Mundial para este tipo de proyectos de inversión.

Se incluye un 25% del costo de los equipos para reinversión en renovación de equipos en el tercer año por su vida útil, en equipos como: tarjetas de *switches* y ruteadores, *access points*, *gateways IP*, cables, etc.

Para la selección de las alternativas se consideran los resultados de rentabilidad obtenidos:

Indicadores de Rentabilidad	VAN US \$	TIR %
Solución 1	117.770,22	53,62
Solución 2	47.257,25	23,38

Tabla 4-39: Indicadores de Rentabilidad de las Soluciones

De los resultados obtenidos se evidencia que la alternativa 1 es rentable para la empresa ya que es aquella de menor costo, que asegura los mismos beneficios de la alternativa 2.

4.2.5 SELECCIÓN DE LA SOLUCIÓN

En base al análisis anterior se recomienda implementar la solución 1, correspondiente a la marca 3COM. Estos equipos cumplen con todas las características técnicas requeridas por este diseño. Adicionalmente son totalmente compatibles con los equipos *Cisco* con los que trabajan los proveedores de *Internet*, como es el caso de Punto Net que maneja una plataforma *Cisco* para brindar servicios tanto de *Internet* como de datos.

La telefonía *IP* propuesta en la solución de 3COM es una central telefónica 3COM *Asterisk*; *Asterisk* es un *software* para la implementación de centrales telefónicas en servidores *Linux* de código abierto. 3COM *Asterisk* funciona bajo el estándar *SIP* que garantiza la compatibilidad de teléfonos de otros fabricantes; para este diseño se utilizó teléfonos *IP* 3COM para mayor compatibilidad.

Las dos soluciones sugieren los equipos para videoconferencia en marca *DLINK*, estos equipos cumplen con los requerimientos del diseño y están diseñados para Latinoamérica de acuerdo a las capacidades de transmisión reducidas, en comparación a Estados Unidos o Europa.

El equipo *3COM* que se utiliza para la seguridad de la red de cada sucursal es un sistema unificado de seguridad que integra: *firewall*, *IPS*, administrador de ancho de banda, inicia y termina *VPNs*, filtro de contenido, eliminación de *malware* y asilamiento de *PCs* infectados a una *VLAN* de aislamiento.

El *software* de administración de red *3COM Network Director* es un completo sistema que brinda opciones avanzadas de configuración y administración de equipos *3COM*. Pero adicionalmente es compatible con cualquier marca de equipos de conectividad que sean compatibles con *SNMP*. *3COM Network Director* puede administrar una red de una pequeña a una mediana empresa, que tenga menos de 100 equipos de conectividad, que es más que suficiente para la realidad de Tecnomega.

3COM Network Director incluye gratuitamente *3COM Network Access Manager*, que es un sistema de administración de usuarios que se integra totalmente a *Active Directory* de *Microsoft*. *3COM Network Access Manager* asocia configuración de los equipos con la administración de los usuarios, es decir se puede configurar un *switch* para que cuando se conecta a la red determinado computador se le asigne a una *VLAN* determinada mediante su dirección *MAC*; permite también configurar su nombre de usuario y contraseña de ingreso a la red por su integración con *Active Directory* y el servidor *RADIUS*.

CAPÍTULO 5
CONCLUSIONES Y
RECOMENDACIONES

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El rediseño del direccionamiento *IP* conjuntamente con la implementación de *VLANs*, mejora el rendimiento de la red al reemplazar la red clase B que se tenía en las sucursales de Quito, con redes clase C para cada sucursal logrando segmentar el dominio de *broadcast*. Las redes clase C de cada sucursal fueron segmentadas en subredes, cada una de ellas maneja una *VLAN* con funciones específicas como: Telefonía *IP*, *Stack* de *switches* (en las sucursales donde existe un *stack* de *switches*). El direccionamiento *IP* de las sucursales de Guayaquil también sigue el mismo esquema que el de Quito.
- Los enlaces entre las sucursales existentes en Quito, tienen la suficiente capacidad para ejecutar las aplicaciones existentes y las sugeridas en este proyecto; por esta razón se pueden utilizar estos enlaces existentes. Para la ciudad de Guayaquil se especifica la capacidad entre las sucursales Mayor y Sur de Guayaquil. El enlace entre Quito y Guayaquil también especifica la capacidad requerida, éste debe ser contratado con un proveedor ya que tiene mucha distancia y sería mucho más caro implementarlo que alquilarlo.
- Todos los enlaces entre sucursales deben implementar *VPNs* para transportar información de la empresa, especialmente los enlaces inalámbricos por la facilidad de interferencia que presentan los mismos. Los equipos que conformen enlaces inalámbricos entre sucursales deben cumplir con los esquemas de seguridad inalámbrica tales como:
 - Todos los equipos deben tener una clave segura para acceder a su configuración.
 - No se debe dejar un equipo con la configuración por defecto.

- Manejar esquemas de encriptación para equipos inalámbricos.
 - Los *SSID* de los equipos inalámbricos no deben ser difundidos para que el enlace sea más seguro.
 - Se deben establecer restricciones de acceso mediante direcciones *MAC* a los equipos inalámbricos de los enlaces entre sucursales.
- La empresa al momento no maneja políticas de seguridad, por lo que ha tenido problemas de pérdida de información de las bases de datos, accesos no autorizados a la red y problemas de virus. Las políticas de seguridad sugeridas en este proyecto se han diseñado en base a los problemas que han surgido y también en base a modelos de políticas de seguridad aplicables a empresas que manejen activos informáticos. La implementación de estas políticas de seguridad, normará los procedimientos que se deben seguir para mitigar lo más posible las vulnerabilidades existentes y determinar las multas por su incumplimiento; se tendrá éxito su implantación si se capacita al personal y se nombra responsables de hacerlas cumplir.
 - Las capacidades de transmisión de los enlaces a *Internet* fueron contratadas sin un estudio previo de dimensionamiento, ocasionando molestias en los usuarios por la lentitud de este servicio; adicionalmente, esto es provocado por la falta de administración de este servicio, porque algunos usuarios instalan gestores de descargas o programas *P2P* y están descargando programas, videos, etc., colapsando la capacidad disponible. Para mejorar los tiempos de respuesta en la carga de páginas *web* y otras aplicaciones que se ejecutan en *Internet* se dimensionó la capacidad necesaria del enlace a *Internet* y se sugiere la instalación de un equipo para administrar la capacidad de este servicio por usuario (administrador de ancho de banda).
 - Las redes convergentes disminuyen costos de mantenimiento ya que eliminan la necesidad de tener una red para telefonía y otra para

datos. Las redes convergentes en una misma red manejan voz, datos y video; ahorrando cableado estructurado mediante *switches* integrados en los teléfonos *IP*. También disminuyen tiempos y costos de solución de problemas porque un sistema de administración de red detecta problemas y facilita su solución en un menor tiempo.

- La implementación de *VLANs* puede ser muy útil o perjudicial para la red, sino se toma en cuenta el esquema de tráfico. Si diseñando las *VLANs* se tiene un tráfico 80% dentro y 20% hacia afuera, es positivo implementarlas; pero si se diseñando las *VLANs* para un tráfico interno del 20% y hacia afuera 80%, es perjudicial para el rendimiento de la red porque todo el tráfico tiene que pasar entre *VLANs* utilizando más recursos de *switches* y ruteadores para su conmutación.
- El códec utilizado para la telefonía *IP* interna en la sucursal es *G.711* para dar prioridad a la calidad de voz, ya que en una red *LAN* el impacto de la capacidad de transmisión de este códec de 64 *Kbps* no es tan importante. Para la telefonía *IP* entre sucursales o por *Internet* se utilizará un códec *G.729* a 8 *Kbps* que mantiene una buena calidad de voz y ocupa una capacidad de transmisión ocho veces menor que *G.711*.
- Se ha reutilizado todas las estaciones de trabajo, servidores y equipos de conectividad utilizados para la implementación de los enlaces entre las sucursales de Quito. Estos equipos tienen una vida útil y todavía están vigentes, están de acuerdo a las aplicaciones que se manejan en la *Intranet*.
- El *software* empresarial se mantiene ya que ha sido desarrollado a medida de la empresa y aun se siguen haciendo modificaciones según los nuevos requerimientos que surgen. Las aplicaciones que se ejecutan sobre *Internet*, también se mantienen porque están totalmente ligadas al SIAC y cumple con todas las expectativas actuales de la empresa.

5.2 RECOMENDACIONES

- Difundir y capacitar al personal de la empresa para cumplir todas y cada una de las políticas de seguridad vigentes. Asignar los empleados responsables de hacer cumplir las políticas de seguridad, así como determinar los montos de las sanciones económicas.

- Las centrales telefónicas de la empresa no estaban interconectadas entre sí, para llamar a otra sucursal se tiene que llamar mediante Andinatel o Pacifictel. Para disminuir costos en llamadas entre sucursales se sugiere un sistema de telefonía *IP* utilizando los enlaces entre las sucursales para interconectar las centrales telefónicas *IP* de la empresa. Además la telefonía *IP* tiene algunas ventajas, como:
 - Cualquier empleado que esté fuera de su oficina si tiene una conexión de *Internet* puede recibir llamadas y revisar sus mensajes de voz.
 - Disminuir costos entre llamadas entre sucursales de la empresa en el país y fuera del mismo. Las llamadas entre sucursales dentro del país utilizan la infraestructura de los enlaces entre sucursales y las llamadas a la sucursal en Estados Unidos se realizarán mediante *Internet*.

- Se recomienda complementar este proyecto con el diseño del cableado estructurado, así como los cuartos de telecomunicaciones de cada una de las sucursales de la empresa. Cumpliendo con los requerimientos para la implementación del mismo.

- Implementar un cuarto de telecomunicaciones en cada una de las sucursales de la empresa, ya que las sucursales no son tan grandes y ningún punto de red está a más de 100 metros de donde debería ir ubicado el cuarto de telecomunicaciones.

- Para complementar las facilidades que brinda un sistema PoE, se debe dimensionar la capacidad del sistema de UPS necesario para garantizar el funcionamiento continuo en caso de apagones.
- Los cuartos de telecomunicaciones deben tener un estricto control de acceso para garantizar el funcionamiento correcto de los equipos y su seguridad física.
- Todos los puntos de red deben cumplir con las normas respectivas de cableado estructurado, los cables deben estar contenidos en tubos *conduit* o canaletas según sea el caso, adicionalmente se recomienda documentar todos los puntos para administrar de una mejor forma la infraestructura.
- Al manejar teléfonos *IP* que necesitan de energía eléctrica se realizó el diseño utilizando *PoE* que utiliza el cable *Ethernet* para transportar energía eléctrica para teléfonos *IP* y *access points*, permitiendo centralizar el suministro eléctrico, mediante sistemas de *UPS* se puede garantizar la continuidad de funcionamiento del Sistema de Telefonía *IP*, aun cuando se tenga un apagón.
- Se recomienda evaluar la red, los enlaces de datos y la salida a *Internet* una vez implementada ejecutando todas las aplicaciones y servicios para los cuales fue rediseñada, monitoreando los equipos y los enlaces para según esto incrementar capacidades de transmisión o realizar los correctivos pertinentes.
- Los fabricantes de equipos de conectividad ofrecen extensiones de garantías, o servicios de reposición de equipos diferentes tiempos, según la importancia de estos en la red. Se recomienda contratar extensiones de garantía de los equipos por el tiempo de vida del proyecto, contratar un servicio de reposición de equipos en horas después del daño si es un equipo de misión crítica y si no lo es puede reponerse el siguiente día laborable a la falla.

- Es muy importante detallar los Acuerdos de Nivel de Servicio (*SLA*) en los contratos de los enlaces entre sucursales y de salida a *Internet*, para desde un principio tener bien claro el tipo de servicio contratado. Y poder verificar que se estén cumpliendo los *SLA* mediante el monitoreo continuo del enlace.
- Se recomienda elaborar un plan de contingencia para disminuir al máximo posible el tiempo fuera de operaciones de la empresa en caso de un incendio, inundación, etc. Lo principal es que las demás sucursales sea afectadas y puedan funcionar a pesar del desastre.
- Se recomienda que la actualización de los sistemas de bases de datos de SQL Server 7.0 no se realice a la versión 2000 porque ya no se encuentra vigente, sino que la actualización se haga a la versión 2005 que está vigente.

REFERENCIAS BIBLIOGRÁFICAS

- TANENBAUM, Andrew, Redes de Computadoras, Cuarta Edición, Editorial Pearson Educación, México, 2003.
- DAVIES, Joseph, Deploying Secure 802.11 Wireless Networks with Microsoft Windows, Editorial Microsoft Press, Washington – EEUU, 2004.
- STALLINGS, William, Local & Metropolitan Area Networks, Quinta Edición, Editorial Prentice Hall, 1997.
- SÁNCHEZ, Tarquino, Material de apoyo para Formulación, Gestión y Evaluación de Proyectos, Quito – Ecuador, 2006.
- HIDALGO LASCANO, Pablo William, Material de apoyo para Redes de Área Local, Quito – Ecuador, 2005.
- HIDALGO LASCANO, Pablo William, Material de apoyo para Redes de Área Extendida, Quito – Ecuador, 2005.
- SINCHE, Soraya, Material de apoyo para Redes de Área Local Inalámbricas, Quito, 2006.
- ÁVILA, Nelson, Material de apoyo para Seguridades en Redes, Quito, 2006.
- CALDERÓN, Xavier, Material de apoyo para Administración de Redes, Quito, 2006.
- <http://www.hyperlinktech.com/web/hg2424g.php>
- <http://www.trendnet.com/sp/products/TEW-410APBplus.htm>
- <http://www.trendnet.com/sp/products/TEW-450APB.htm>
- <http://lat.3com.com/lat/>
- <http://www.cnet.com.tw/product/cgs-800.htm>
- <http://www.microsoft.com/technet>
- www.cisco.com
- www.panasonic.com
- http://www.evdocs.com/index.php?page=index_v2&id=163&c=10
- <http://www.zonagratis.com/servicios/seguridad/puertoswin2000.html>
- <http://sd.wareonearth.com/~phil/net/overhead/>

- [http://www.trendcomms.com/trendweb/resource.nsf/vlFileURLLookup/Metro.Ethernet/\\$FILE/Metro.Ethernet.pocket.pdf](http://www.trendcomms.com/trendweb/resource.nsf/vlFileURLLookup/Metro.Ethernet/$FILE/Metro.Ethernet.pocket.pdf)
- www.tecnomega.com
- www.interactive.net.ec
- www.wikipedia.org
- <http://www.microsoft.com/latam/technet/techinfo/intranet/default.asp>
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
- www.alliedtelesyn.com
- www.dlinkla.com